PATENT ABSTRACTS OF JAPAN

(11)Publication number : **11-143833**

(43)Date of publication of application : **28.05.1999**

(51)Int.CI. **G06F 15/00**

G09C 1/00

H04L 9/32

(21)Application number : **09-313390**

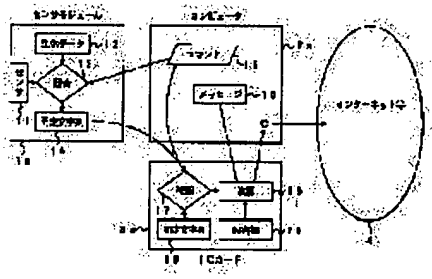
(22)Date of filing : **14.11.1997**

(71)Applicant : **TOSHIBA CORP**

(72)Inventor : **YAMADA KOUKI**

(54) USER CONFIRMATION SYSTEM AND IC CARD BY BIOLOGICAL DATA AND STORAGE MEDIUM

(57)Abstract:



PROBLEM TO BE SOLVED: To make it possible to protect biological data with high safety by putting them in a management range at hand of a user and to reduce a feeling of resistance and a risk of leakage of the biological data.

SOLUTION: This user confirmation system consists of a sensor 11 for performing a biological measurement, a biological data holding part 12 for holding biological data, a tamper proof sensor module 1a that is equipped with a collating calculation part 13 which collates measurement information measured by the sensor with the biological data in the biological data holding part and outputs a notification of the fact when a person concerned is confirmed by the collated result, an IC card 3a that performs a data output by corresponding to that a user confirmation is made when the notification is received, a confirmation processing part 17, an operation processing part 19 and a communication means 2a for performing a communication between the sensor module and the IC card.

LEGAL STATUS

[Date of request for examination] 18.09.2000

[Date of sending the examiner's decision of rejection]	13.07.2004
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	
[Date of registration]	
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

CLAIMS

[Claim(s)]

[Claim 1] While collating the measurement information measured by said sensor, and the living body data of said living body data-hold circles with the living body data-hold section holding the sensor which performs somatometry, and living body data, and a list The sensor module of the tamper-proof nature equipped with the collating count section which outputs a notice to that effect when checked with him from a collating result, The user check system by the living body data characterized by consisting of means of communications which performs the communication link between the IC card which performs data output made corresponding to the user check having been carried out, and said sensor module and said IC card if said notice is received.

[Claim 2] While collating the sensor module equipped with the sensor which performs somatometry, and the measurement information measured by the living body data-hold section holding living body data, and said sensor and the living body data of said living body data-hold circles If said notice is received in the collating count section and the list which output a notice to that effect when checked with him from a collating result The user check system by the living body data characterized by consisting of means of communications which performs the communication link between the IC card of the tamper-proof nature equipped with the data-processing section which performs data output made corresponding to the user check having been carried out, and said sensor module and said IC card.

[Claim 3] While collating the measurement information measured by the decode section which receives the sensor which performs somatometry, and the enciphered living body data, and decrypts this, and the list by said sensor, and said decrypted living body data When checked with him from a collating result, while holding the sensor module equipped with the collating count section which outputs a notice to that effect, and said enciphered living body data If the notice from said collating count section is received in the living body data-hold section and the list which send out the enciphered living body data concerned to said sensor module The user check system by the living body data characterized by consisting of means of communications which performs the communication link between the IC card of the tamper-proof nature equipped with the data-processing section which performs data output made corresponding to the user check having been carried out, and said sensor module and said IC card.

[Claim 4] The user check system by the living body data according to claim 3 characterized by giving tamper-proof nature to said sensor module.

[Claim 5] While collating the sensor module equipped with the sensor which performs somatometry, the measurement information measured by the decode section which receives the enciphered living body data and decrypts this, and the list by said sensor, and said decrypted living body data When checked with him from a collating result, while holding the computer equipped with the collating count section which outputs a notice to that effect, and said enciphered living body data If the notice from said collating count section is received in the living body data-hold section and the list which send out the enciphered living body data concerned to said computer The IC card of the tamper-proof nature equipped with the data-processing section which performs data output made corresponding to the user check having been carried out, The user check system by the living body data characterized by consisting of means of communications which performs the communication link between said sensor modules, said IC cards, and said computers.

[Claim 6] said IC card -- a user -- claim 1 characterized by containing the digital signature by said signature means in the data output made corresponding to having had a signature means to perform his digital signature, and said user check having been carried out thru/or the user check system according to living body data any or given in 1 term among 5.

[Claim 7] the sensor module equipped with the sensor which performs somatometry, and a user -- the living body data enciphered by his log on password The living body data-hold section held as information which shows that the user concerned has the authority corresponding to a user demand, When said user demand and said log on password are inputted into a list, while decrypting the living body data of said living body data-hold section by said log on password When the measurement information measured by this decrypted living body data and said sensor is collated and he and authority are checked by that collating result The user check system by the living body data characterized by consisting of means of communications which performs the communication link between the computer equipped with the collating count section which outputs the notice of a purport which should carry out said user demand, and said computer and said sensor module.

[Claim 8] In the user check system which performs data encryption processing while consisting of the sensor which performs somatometry, a computer, and an IC card and performing a user check said IC card The living body data-hold section which has tamper-proof nature and holds living body data, The 1st code count section in said data encryption processing which performs processing in part, The list is equipped with the cryptographic key attaching part holding the cryptographic key used for processing in said 1st code count section at least. Said computer It has at least the 2nd code count section which will perform other processings in said data encryption processing if the notice of a user check is received. Furthermore, while collating the measurement information measured by said sensor, and the living body data of said living body data-hold circles The user check system by the living body data characterized by consisting of a collating count means to output said notice of a user check to said 2nd code count section when checked with him from a collating result, and means of communications which performs the communication link between said sensors, said IC cards, and said computers.

[Claim 9] a computer -- a user -- with the living body data-hold function which shows that the user concerned has the authority corresponding to a user demand for the living body data enciphered by his log on password and which is held as information When said user demand and said log on password are inputted, while decrypting said living body data by said log on password When the measurement information by which somatometry was carried out to this decrypted living body data is collated and he and authority are checked by that collating result The record medium which recorded the program for realizing the collating count function which outputs the notice of a purport which should carry out said user demand and in which computer reading is possible.

[Claim 10] When the notice of a user check is received in a computer While performing processing in part, from the exterior reception and its processing result for the processing result of other processings in this data encryption processing in data encryption processing Said code count function for processing to use a part and to complete encryption processing, While collating the measurement information and the living body data for a user check by which somatometry was carried out a collating result -- a user -- the record medium which recorded the program for realizing the collating count function to perform said notice of a user check on said code count function when checked with him and in which computer reading is possible.

[Claim 11] A living body data-hold means to output this enciphered living body data to an external device while holding the enciphered living body data, the measurement information by which somatometry was carried out to said living body data -- a user, if the collating result of the purport checked with him is notified from said external device The IC card characterized by having a data-processing means to perform data output made corresponding to the user check having been carried out, and having tamper-proof nature.

[Claim 12] Said external device is an IC card according to claim 11 characterized by being the sensor module which has the sensor which performs somatometry.

[Claim 13] Said external device is an IC card according to claim 11 characterized by being a computer.

[Claim 14] said data-processing means -- a user -- claim 11 characterized by containing the digital signature by said signature means in the data output made corresponding to having had a signature means

to perform his digital signature, and said user check having been carried out thru/or the inside of 13 -- an IC card any or given in 1 term.

[Claim 15] a living body data-hold means to output said living body data to the external device which performs a user check using this living body data while holding living body data, and the part in data encryption processing, while performing processing using a cryptographic key The IC card characterized by equipping the external device which performs other processings in this data encryption processing with said code count means to output the processing result of processing in part, and a cryptographic key maintenance means to hold said cryptographic key, and having tamper-proof nature.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

TECHNICAL FIELD

[Field of the Invention]

[0001] This invention relates the digital signature processing using an IC card, the use authority check of calculating-machine software or the use authority check of data encryption processing, etc. to a record medium at convenient, the user check system by the living body data for carrying out to insurance, and an IC card list.

PRIOR ART

[Description of the Prior Art]

[0002] The magnetic card is mainly used to check a user from the former for the credit card, the close leaving managed card, etc. On the other hand, the effectiveness which prevents forgery and an information leak of a card is expected, and a highly efficient IC card is beginning to be used recently with the high security which built in the semiconductor chip.

[0003] However, even if it uses an IC card, it is difficult to prevent it to being used improperly by others according to loss or a theft, or a false using improperly as loss.

[0004] Although it is performed that it is going to reduce an unauthorized use by registering the password corresponding to an IC card, as for a password, memorizing is troublesome, and there are a danger of forgetting, and a danger of it being read by others and revealing a memorandum, and it can never be said that it is convenient.

[0005] recently -- a fingerprint and a palm -- there is a motion which is going to perform close leaving management and an access control combining the biometrics and the IC card which are the technique of measuring living body data like type and checking him. It is thought that the various problems produced by loss of a card, the theft, leakage, oblivion, etc. are solved by this.

[0006] However, a user's feeling [/ that only / not a thing like a password that can be created freely but / the information on its body (living body data) is registered into somewhere by one side] of resistance, and a user's insecurity over the weak spot where modification like a password is not effective when it is revealed, and a leakage trouble remain firmly. [best] Therefore, to use biometrics for a user check, it is necessary to build the system which proposes a technique whose above-mentioned feeling of resistance decreases, and can prevent leakage of living body data effectively.

[0007] Furthermore, in the environment where the use authority check of calculating-machine software with usually not using [much] an IC card is performed, there is no medium which holds living body data safely, and when using biometrics, living body data must be stored on the storage of a calculating machine. However, there is a danger that living body data will be revealed with reverse engineering in this case.

TECHNICAL PROBLEM

[Problem(s) to be Solved by the Invention]

[0008] As mentioned above, with the technique which uses together a conventional IC card and a conventional password, there is a trouble of the danger of troublesomeness, oblivion, or leakage.
[0009] Moreover, in concomitant use of an IC card and biometrics, the feeling of resistance of the information on its body (living body data) being registered and the danger that living body data will be revealed to a third person remain.

[0010] Furthermore, when use authority was checked in the environment where an IC card is not used, using biometrics, there was no approach of recording living body data on insurance.

[0011] it make it possible to have make this invention in consideration of the above-mentioned situation , to be able to put it on the management range of a user hand as it be also at high safety about living body data , to be able to protect it , as a result to reduce a user's feeling of resistance , and the leakage danger of living body data , and aim at provide the user check system and IC card list by living body [with the high certainty of a user check] data with little troublesomeness on use with a record medium further .

MEANS

[Means for Solving the Problem]

[0012] In order to solve the above-mentioned technical problem, invention corresponding to claim 1 While collating the measurement information and the living body data of living body data-hold circles which were measured by the sensor with the living body data-hold section holding the sensor which performs somatometry, and living body data, and a list The sensor module of the tamper-proof nature equipped with the collating count section which outputs a notice to that effect when checked with him from a collating result, When a notice is received, it is a user check system by the living body data which consist of means of communications which performs the communication link between the IC card which performs data output made corresponding to the user check having been carried out, and a sensor module and an IC card.

[0013] since this invention established such a means, while the living body data of living body data-hold circles are protected by the sensor module of tamper-proof nature, being able to protect that it is also at high safety about living body data and reducing the leakage danger of living body data -- further -- the troublesomeness on use -- few -- carrying out -- a user -- him -- certainty of a check can be made high.

[0014] Next, while invention corresponding to claim 2 collates the sensor module equipped with the sensor which performs somatometry, and the measurement information and the living body data of living body data-hold circles which were measured by the living body data-hold section holding living body data, and the sensor If a notice is received in the collating count section and the list which output a notice to that effect when checked with him from a collating result It is a user check system by the living body data which consist of means of communications which performs the communication link between the IC card of the tamper-proof nature equipped with the data-processing section which performs data output made corresponding to the user check having been carried out, and a sensor module and an IC card.

[0015] Since such a means was established, the same effectiveness as invention corresponding to claim 1 is acquired, and also by having prepared in the IC card of tamper-proof nature, the living body data-hold section can be put on the management range of a user hand as it is also at high safety about living body data, and this invention can protect it, as a result can reduce a user's feeling of resistance.

[0016] Next, while invention corresponding to claim 3 collates the measurement information measured by the decode section which receives the sensor which performs somatometry, and the enciphered living body data, and decrypts this, and the list by the sensor, and the decrypted living body data When checked with him from a collating result, while holding the living body data enciphered as the sensor module equipped with the collating count section which outputs a notice to that effect If the notice from the collating count section is received in the living body data-hold section and the list which send out the enciphered living body data concerned to said sensor module It is a user check system by the living body data which consist of means of communications which performs the communication link between the IC card of the tamper-proof nature equipped with the data-processing section which performs data output made corresponding to the user check having been carried out, and a sensor module and an IC card.

[0017] Since this invention established such a means, the same effectiveness as invention corresponding to claim 2 can be acquired.

[0018] Moreover, invention corresponding to claim 4 is a user check system by the living body data which gave tamper-proof nature to the sensor module in invention corresponding to claim 3.

[0019] Since this invention established such a means, it can acquire the same effectiveness as invention corresponding to claim 3, and also it can raise the safety of living body data etc. further.

[0020] Furthermore, the sensor module equipped with the sensor by which invention corresponding to claim 5 performs somatometry, While collating the measurement information measured by the decode section which receives the enciphered living body data and decrypts this, and the list by the sensor, and the decrypted living body data When checked with him from a collating result, while holding the living body data enciphered as the computer equipped with the collating count section which outputs a notice to that effect If the notice from the collating count section is received in the living body data-hold section and the list which send out the enciphered living body data concerned to a computer It is a user check system by the living body data which consist of means of communications which performs the communication link between the IC card of the tamper-proof nature equipped with the data-processing section which performs data output made corresponding to the user check having been carried out, a sensor module and an IC card, and a computer.

[0021] Since this invention established such a means, while a certain extent is obtained in the same effectiveness as invention corresponding to claim 2, a simple and cheap system can be built.

[0022] invention corresponding to claims 1-5 in invention corresponding to [further again] claim 6 -- setting -- an IC card -- a user -- it is a user check system by the living body data with which the digital signature by the signature means is contained in the data output made corresponding to having had a signature means to perform his digital signature, and the user check having been carried out.

[0023] Since this invention established such a means, the same effectiveness as invention corresponding to claims 1-5 is acquired, and also the digital signature system using an IC card can be built.

[0024] The sensor module equipped with the sensor by which invention corresponding to claim 7 performs somatometry on the other hand, a user -- the living body data enciphered by his log on password The living body data-hold section held as information which shows that the user concerned has the authority corresponding to a user demand, When a user demand and a log on password are inputted into a list, while decrypting the living body data of the living body data-hold section by the log on password When the measurement information measured by this decrypted living body data and sensor is collated and he and authority are checked by that collating result It is a user check system by the living body data which consist of means of communications which performs the communication link between the computer equipped with the collating count section which outputs the notice of a purport which should carry out a user demand, and a computer and a sensor module.

[0025] Since this invention established such a means, the living body data enciphered with the password can keep the secret, even if it reveals independently, and can also keep the use authority of software. moreover, the user using biometrics -- him -- since a check and an authority check are made -- the troublesomeness on use -- few -- carrying out -- a user -- him -- certainty of a check can be made high.

[0026] Moreover, invention corresponding to claim 8 is set to the user check system which performs data encryption processing while consisting of the sensor which performs somatometry, a computer, and an IC card and performing a user check. The living body data-hold section which an IC card has tamper-proof nature, and holds living body data, The 1st code count section in data encryption processing which performs processing in part, The list is equipped with the cryptographic key attaching part holding the cryptographic key used for processing in the 1st code count section at least. A computer If the notice of a user check is received, while having at least the 2nd code count section which performs other processings in data encryption processing and collating further the measurement information and the living body data of living body data-hold circles which were measured by the sensor When checked with him from a collating result, it is a user check system by the living body data which consist of a collating count means to output the notice of a user check to the 2nd code count section, and means of communications which performs the communication link between a sensor, an IC card, and a computer.

[0027] since this invention established such a means, living body data and a cryptographic key store in the high IC card of tamper-proof nature -- having -- a trustworthy user -- him -- encryption processing can be performed after a check is made. Moreover, since he is trying for an IC card and a computer to share encryption processing, high encryption of secrecy nature is extremely realizable.

[0028] furthermore, invention corresponding to claim 9 -- a computer -- a user -- the living body data enciphered by his log on password When a user demand and a log on password are inputted as the living body data-hold function which shows that the user concerned has the authority corresponding to a user demand and which is held as information, while decrypting living body data by the log on password When the measurement information by which somatometry was carried out to this decrypted living body data is collated and he and authority are checked by that collating result It is the record medium which recorded the program for realizing the collating count function which outputs the notice of a purport which should carry out a user demand and in which computer reading is possible.

[0029] Since this invention established such a means, actuation of the computer in the user check system by the living body data indicated to claim 7 can be realized.

[0030] When the notice of a user check is received in a computer, invention corresponding to claim 10 further again The code count function to complete encryption processing for the processing result of processing of the others in this data encryption processing in data encryption processing while performing

processing in part using reception and its processing result from the exterior, while collating the measurement information and the living body data for a user check by which somatometry was carried out -- a collating result -- a user -- when checked with him, it is the record medium which recorded the program for realizing the collating count function to perform the notice of a user check on the code count function and in which computer reading is possible.

[0031] Since this invention established such a means, actuation of the computer in the user check system by the living body data indicated to claim 8 can be realized.

[0032] On the other hand, while invention corresponding to claim 11 holds the enciphered living body data A living body data-hold means to output this enciphered living body data to an external device, the measurement information by which somatometry was carried out to living body data -- a user, if the collating result of the purport checked with him is notified from an external device It is the IC card characterized by having a data-processing means to perform data output made corresponding to the user check having been carried out, and having tamper-proof nature.

[0033] Since this invention established such a means, actuation of the IC card in the user check system by the living body data indicated to claim 3 or 5 can be realized.

[0034] Next, in invention corresponding to claim 11 in invention corresponding to claim 12, an external device is an IC card which is the sensor module which has the sensor which performs somatometry.
[0035] Since this invention established such a means, actuation of the IC card in the user check system by the living body data indicated to claim 3 or 4 can be realized.

[0036] Moreover, invention corresponding to claim 13 is an IC card whose external device is a computer in invention corresponding to claim 11.

[0037] Since this invention established such a means, actuation of the IC card in the user check system by the living body data indicated to claim 5 can be realized.

[0038] furthermore, invention corresponding to claims 11-13 in invention corresponding to claim 14 -- setting -- a data-processing means -- a user -- it is the IC card with which the digital signature by the signature means is contained in the data output made corresponding to having had a signature means to perform his digital signature, and the user check having been carried out.

[0039] Since this invention established such a means, actuation of the IC card in the user check system by the living body data which also have the means of claim 6 further among invention corresponding to claims 3-5 can be realized.

[0040] Moreover, while invention corresponding to claim 15 holds living body data a living body data-hold means to output living body data to the external device which performs a user check using this living body data, and the part in data encryption processing, while performing processing using a cryptographic key It is the IC card which is equipped with a code count means to output the processing result of processing to the external device which performs other processings in this data encryption processing in part, and a cryptographic key maintenance means to hold a cryptographic key, and has tamper-proof nature.

[0041] Since this invention established such a means, actuation of the IC card in the user check system by the living body data indicated to claim 8 can be realized.

EXAMPLE

[Embodiment of the Invention]

[0042] Hereafter, the gestalt of operation of this invention is explained.

[0043] As already stated, this invention aims at reducing a user's feeling of resistance to reducing the leakage danger of 1 living body data, and storing information machines and equipment for the living body data of 2 selves, and offers a means by which both both [either or] 1 and 2 is realizable.

[0044] Especially artificers examined many things about whether the above-mentioned purpose is realizable, when making biometrics apply to the IC card signature system as one gestalt of the user check system by living body data and building what kind of system. Here, an IC card signature system is a system which an IC card with the function to operate the digital signature function inside an IC card is used [system], and realizes shopping on sending by the electronic mail of extra sensitive information, and the Internet etc. by the digital signature. the case where biometrics is made to apply to this system -- a collating result with the sensor measurement information about living body data, such as a fingerprint, -- being based -- him -- it checks and the above-mentioned digital signature function of an IC card is made to operate on it

[0045] Artificers examined four modules, i.e., an IC card, the sensor module, the computer (PC, IC card reader / writer ****), and the server as an element which can first constitute the IC card signature system (only henceforth an IC card signature system or a system) to which biometrics was made to apply. Next, when which module performed processing (living body (registration) data logging, collating count) performed in an IC card signature system, respectively, it examined whether the purpose of this invention could be attained.

[0046] Drawing 15 is drawing showing the component in the IC card signature system to which biometrics was made to apply, and its combination result.

[0047] Priority is given to performing the owner check of an IC card by local processing in consideration of the user who dislikes registering with the central processing unit no living body data are [central processing unit] to a user among each candidate system shown in drawing 15 existing. Therefore, the thing using a server was excepted at this time of examination. It is because it will be thought that a user's feeling of resistance can be reduced if it is the system which can put living body data on the management range of a user hand, and can protect them. However, if in interpreting invention which is fruition of a technical result it is within the limits indicated by the claim when satisfactory [especially concerning the above-mentioned feeling of user resistance], the technique of using a server etc. is also included in the invention range.

[0048] Next, in consideration of usable in the same terminal (a sensor, PC) at many and unspecified persons, and convenience usable at a terminal further unspecified in the same person, it left as a candidate system what holds living body data to an IC card.

[0049] In addition, what set living body data-hold and the collating count section in one module of tamper-proof nature (an IC card or sensor module) considered as the candidate, and left. In this case, it is because the communication link between the living body data - collating count sections becomes unnecessary, a protocol becomes simple and security can also be made high. Here, tamper-proof nature is a property with the structure which cannot take out the object or information on internal outside easily with the original form. Although various approaches can be considered to realize this tamper-proof nature, about the concrete example of that approach, it mentions later.

[0050] In this way, as shown in drawing 15, five candidate systems especially considered to be effective out of much combination were found out. In addition, among this drawing, it is the identification code for performing device authentication between an IC card, PC, etc. which was described as "PIN", and it has distinguished the signature key.

[0051] Invention hereafter made corresponding to the candidate system shown in drawing 15 is explained in the 5th operation gestalt from the 1st operation gestalt, and the alien system which is not shown in this drawing is further explained in the 8th operation gestalt from the 6th operation gestalt.

[0052] (Gestalt of implementation of the 1st of invention) Drawing 1 is the block diagram showing an example of the user check system by the living body data concerning the gestalt of operation of the 1st of this invention.

[0053] This user check system is tamper-proof module one apparatus of the candidate systems of drawing 15, and consists of sensor module 1a, computer 2a, and IC card3a. By this system, collating count is performed with living body data-hold by the sensor module 1a side, and sensor module 1a which performs only signature processing consists of a sensor 11, the living body data-hold section 12, the collating processing section 13, and the identification character string storing section 14 at the IC card 3a side. In addition, although not illustrated especially, CPU, memory, etc. are built in this sensor module 1a, and it has become it as [perform / various information processing].

[0054] Here, a sensor 11 is a means which measures a fingerprint as somatometry and is made into electronic information, and each user's living body data are stored in the living body data-hold section 12. moreover, the sensor information and living body data with which the collating count section 13 was measured -- collating -- a user -- while judging whether you are him -- a user -- when it is him, it is a means to notify an output to that effect. In addition, with this operation gestalt, the collating processing section 13 outputs the identification character string (only henceforth a password) of the identification character string storing section 14 to IC card 3a through computer 2a.

[0055] Here, sensor module 1a is a stand-alone type, and has tamper-proof nature. In addition, a stand-alone type has a sensor 11 and the collating count section 13 at least in a tamper-proof sensor module. The security of this system is mainly based on the tamper-proof nature of the living body data in sensor module 1a, and the collating count section 13. For this reason, each part other than sensor 11 in sensor module 1a is constituted by IC of one chip. Moreover, module each component is stored in a firm case, and the lid opens it. Furthermore, if a lid is opened compulsorily, it is the structure by which the IC chip itself in which the living body data-hold section 12, the collating processing section 13, and the identification character string storing section 14 are stored is destroyed. With this operation gestalt, this case was embedded in the wall and the further tamper-proof nature is secured.

[0056] Moreover, it has led to having constituted each part 12, 13, and 14 other than sensor 11 from an IC

of one chip itself securing tamper-proof nature. For example, since information is held as it is on the magnetic tape front face at the magnetic card when password information is stored in a magnetic card, if even the structure of information maintenance is known, the above-mentioned password information can be read easily and tamper-proof nature is low. On the other hand, when it stores information in IC chip, information will be acquired from a terminal only after inputting a command etc. as an electrical signal from the chip terminal. A high technique is required for performing this actuation, and it can be said to be high [tamper-proof nature] that much.

[0057] Moreover, since living body data are used only within the same IC chip in the case of this operation gestalt, the external output of living body data is constituted so that it cannot do, in order the external output is unnecessary and to raise tamper-proof nature.

[0058] In addition, in this specification, when it is said that it has tamper-proof nature, the measure which all the all [above-mentioned / above-mentioned either or] is together put, and others can consider is taken. Moreover, in the case of a sensor module, it explained, but also in the case of an IC card, the same measure can raise tamper-proof nature here. Especially when it is an IC card, for example, if the case is opened, it is also possible to establish structure in which iron powder scatters on wiring and vanishes all maintenance information.

[0059] Moreover, it could be said that there is tamper-proof nature, when considering whether there is only any tamper-proof nature or there is nothing as a minimum argument, and contents to protect, for example are dedicated in one IC chip.

[0060] Next, the command output section 15 and the message output section 16 are formed in computer 2a. Moreover, an IC card reader & writer is contained in computer 2a, and this point is the same also with each following operation gestalt.

[0061] Furthermore, although especially computer 2a does not illustrate, it is possible to execute various application programs, such as a browser, and the Internet 4 is accessed with this operation gestalt.
[0062] It connects with the virtual Mall further and on-line shopping has become possible [from computer 2a] in the Internet 4. The sign "C" shown in computer 2a shows demand outputs, such as goods purchase to a virtual Mall, in the example of this operation gestalt mentioned later of operation, although it is the calculated message (digital signature processing etc.).

[0063] IC card 3a is equipped with the check processing section 17, the identification character string storing section 18, the data-processing section 19, and the private key attaching part 20, and resources which realize these each part, such as CPU and memory, are dedicated to IC of one chip.

[0064] The check processing section 17 notifies the check result to the data-processing section 19 as compared with the identification character string (password) in which the identification character string from sensor module 1a was stored by the identification character string storing section 18 in an IC card. That is, sensor module 1a and IC card 3a will share the identification character string for telling the information on whether he was checked or not from a sensor module in secrecy to an IC card. Specifically, what enciphered the identification character string by the side of a sensor module may be used exactly like [the identification character string by the side of an IC card is the same as that of the identification character string by the side of a sensor module, or] the encryption password in UNIX. Corresponding to the identification character string sent from the sensor module in short, the only identification character string in an IC card corresponds.

[0065] the data-processing section 19 -- a system user -- a user -- if the notice of a check of being him is received from the check processing section 17, predetermined data processing will be performed and the calculated message C will be outputted. The **** message for example, on entrance management is sufficient as this message, and the equipment starting instruction of a computer etc. is sufficient as it. The data-processing section 19 is outputted to the virtual Mall on the Internet here as a message C which calculated the goods purchase demand based on the information on the message output section 16 while it performs a digital signature as a concrete example using the private key stored in the private key attaching part 20.

[0066] Next, actuation of the user check system by the living body data concerning the gestalt of operation of this invention constituted as mentioned above is explained.

[0067] As described above, in various cases, the user check system by living body data is applicable, but the example of operation is explained here taking the case of the case where a goods purchase demand is outputted to the virtual Mall on the Internet.

[0068] Drawing 2 is the flow chart showing the example of this operation gestalt of operation.
[0069] In this example of operation, the personal computer (personal computer) as computer 2a is started in a house or a firm, browser software is started, and the case where it is going to connect with Internet 4 pan in a virtual Mall, and is going to carry out goods purchase is assumed.

[0070] A user makes a selection decision of goods and its purchase quantity in a virtual Mall, and clicks the buy button on a personal computer. As this actuation shows to drawing 1 , a command 15 is outputted to sensor module 1a and IC card 3a from computer 2a, and the display of various directions etc. is made on computer 2a (ST1).

[0071] Here, in IC card 3a not being inserted in a system, the message "insert an IC card" is sent from computer 2a here, and IC card 3a is inserted in it by the user (ST2). In addition, it is notified that goods purchase processing was started from computer 2a to the card 3a concerned in connection with card insertion (command 15).

[0072] Next, if a user presses his finger against the sensor 11 of sensor module 1a, somatometry by the sensor 11 will be performed (ST3).

[0073] Next, if the measured sensor information is collated with living body data in the collating count section 13 of sensor module 1a (ST4) and he is checked (ST5), the identification character string in the identification character string storing section 14 (password) will be outputted to IC card 3a (ST6). In addition, this processing is conventionally replaced with the key input of the password in a system. Moreover, what is necessary is just to encipher in identification character string sending out in IC card 3a from sensor module 1a, instead of sending an identification character string in the flesh, in order to eliminate the danger of tapping of the identification character string by the hacker.

[0074] moreover -- the case where he cannot check in a step ST 5 -- a system user -- a user -- the purport which is not him is displayed and subsequent processings are stopped.

[0075] the identification character string which received compares with the identification character string by which it was held in the card in the check processing section 17 of IC card 3a -- having -- a system user -- a user -- it is checked that he is him (ST7). If a he check is made, that will be notified to the data-processing section 19.

[0076] While Message C is created by the data-processing section 19 which received the notice of a he check based on the goods purchase information from the message output section 16, a digital signature is performed in the message C by the private key held at the private key attaching part 20 (ST8).

[0077] In this way, the message C created and calculated will be outputted to the Internet 4 from computer 2a, and goods purchase in a virtual Mall will be realized.

[0078] As mentioned above, the user check system by the living body data concerning the gestalt of operation of this invention Store the living body data-hold section 12 and the collating count section 13 which performs collating by living body data in the same sensor module 1a, and it is made for living body data not to output out of sensor module 1a. And since high tamper-proof nature was given to the sensor module 1a itself, a user's feeling of resistance to being able to abolish most leakage danger of living body data, as a result storing information machines and equipment for the living body data of self by this can be reduced.

[0079] moreover -- since it faces performing a digital signature etc. and is made to carry out a user check not based on a password input but based on the somatometry to him -- him with very high certainty -- it can check. Even when it followed, for example, an IC card is lost or it is stolen, the improper use by the 3rd person can be prevented.

[0080] Furthermore, in this system, after collating by the collating count section 13, since the result was notified to the data-processing section 19 using the password, it can process safely after checking him until it carries out a digital signature, and an IC card signature system with very high security can be realized. Even if it seems that the whole system which followed, for example, includes an IC card may be stolen, that a theft person gets living body data cannot output the fake message C, either. In addition, in such a case, high tamper-proof nature is given at the IC card 3a itself so that neither a private key nor an identification character string may be revealed.

[0081] Moreover, since biometrics is used in the system of this operation gestalt, it is not necessary to memorize a password etc. and a system without the troublesomeness of a password input or the danger of the oblivion and leakage can be offered.

[0082] Furthermore, with this operation gestalt, since each requirement for a configuration of a sensor 11, the living body data-hold section 12, the collating processing section 13, the identification character string storing section 14, the check processing section 17, the identification character string storing section 18, the data-processing section 19, and the private key attaching part 20 has been arranged to sensor module 1a and IC card 3a as shown in drawing 1 , the merit on IC card use besides each above-mentioned effectiveness is also obtained. That is, the IC card for the conventional signature can be used almost as it is. In the semantics, this operation gestalt can also be said to be an existing card use mold. Since it is not necessary to publish the special IC card put in bearing adoption of fingerprint authentication processing in mind, a system can be immediately introduced only by modification of software. Since there is no collating count section 13 on IC card 3a, the load to an IC card can be made small.

[0083] In addition, in the case of shopping in a virtual Mall, the above-mentioned example of operation explained, but the installation to the purchase demand of SET (Secure Electronic Transaction) can more specifically be considered. Although SET is a specification bearing a magnetic card in mind originally, use of an IC card (+ password) can also be performed as a practical use gestalt. If the technique explained with this operation gestalt is introduced into the processing of "signing with a member's private key" in the verification and the purchase demand by the card member, it will be thought that the usefulness increases.

[0084] moreover, the thing by which this invention is restricted to this although the fingerprint was used as living body data with this operation gestalt -- it is not -- a palm -- also when using various living body data, such as type, a voiceprint, a retina, and a photograph of his face, it can apply. Moreover, since a sensor 11 and the digital signature functional divisions 19 and 20 in an IC card have dissociated, the degree of freedom of the sensor class to be used can be enlarged.

[0085] Furthermore, people are able to enable it to use many same systems only as a personal system in the system of this operation gestalt by two or more living body data being made to be made into the living body data-hold section 12 of sensor module 1a.
(Gestalt of implementation of the 2nd of invention) Drawing 3 is the block diagram showing an example of the user check system by the living body data concerning the gestalt of operation of the 2nd of this invention, it gives the same sign to the same part as drawing 1 , omits explanation, and describes only a part different here.

[0086] This user check system is an omnipotent IC card mold of the candidate systems of drawing 15 , and consists of sensor module 1b, computer 2b, and IC card3b. By this system, in sensor module 1b, only sensor input transmission performs (easy scramble processing is performed), and, in addition to signature processing, performs collating count with living body data-hold at the IC card 3b side.

[0087] The function of the sensor 11 in each configuration shown in drawing 3, the living body data-hold section 12, the collating processing section 13, the check processing section 17, the data-processing section 19, and the private key attaching part 20 is the same as that of what is shown in drawing 1 of the 1st operation gestalt. However, the arrangement locations of each part differ.

[0088] That is, with this operation gestalt, only the sensor 11 is formed in sensor module 1b. On the other hand, the living body data-hold section 12, the collating processing section 13, the check processing section 17, the data-processing section 19, and the private key attaching part 20 are formed in IC card1b, and these are constituted in same IC chip. In addition, the configuration of computer 2b is the same as that of computer 2a of the 1st operation gestalt.

[0089] Although so high tamper-proof nature is unnecessary to sensor module 1b since each part is arranged in this way, high tamper-proof nature is required of IC card3b, and tamper-proof nature is secured with a means which was explained with the 1st operation gestalt.

[0090] Next, actuation of the user check system by the living body data concerning the gestalt of operation of this invention constituted as mentioned above is explained.

[0091] Taking the case of access to the virtual Mall on the Internet 4, it explains also here like the 1st operation gestalt.

[0092] Drawing 4 is the flow chart showing the example of this operation gestalt of operation.

[0093] In this drawing, the processing from a step ST 11 to ST13 is the same as that of the drawing 2 step ST 1 of the 1st operation gestalt to ST3.

[0094] Next, from sensor module 1b, the measured sensor information is sent out to IC card 3b (ST14). In IC card3b which received sensor information, the same collating as processing is performed within sensor module 1a of the 1st operation gestalt (ST15). In addition, since this collating processing is performed only within IC card 3b, in order to raise tamper-proof nature, the living body data of the living body data-hold section 12 have composition which cannot be outputted outside from IC card3b.

[0095] collating -- him -- if a check is made (ST16), the check result will be notified to the data-processing section 19 (ST17), and the message C which calculated by performing a digital signature etc. (ST18) will be outputted to a virtual Mall like the 1st operation gestalt below (ST19).

[0096] As mentioned above, the user check system by the living body data concerning the gestalt of operation of this invention While storing the collating processing section 13 and the living body data-hold section 12 in the same IC card 3b Since tamper-proof nature of the card 3b concerned was made high, while being able to reduce the leakage danger of living body data It can put that it is also at high safety about living body data on the management range of a user hand (IC card), and can protect, and a user's feeling of resistance to storing information machines and equipment for the living body data of self can be reduced sharply. That is, since all main elements other than a sensor are mounted in the IC card which carries out individual possession, sense of security is mentally strong.

[0097] Moreover, since the collating count section 13 and the data-processing section 19 are constituted in same IC chip, it can process safely after checking him until it carries out a digital signature, and an IC card signature system with very high security can be realized.

[0098] Moreover, in the system of this operation gestalt, since only signal processing comparatively primitive in a sensor module side is made to take charge of, the burden of sensor module 1b can be made small.

[0099] To a collating unit, there is no omnipotent IC card mold and it can apply a special request with the fingerprint collation device of every mold. The security of this system is chiefly based on the tamper-proof nature of an IC card, and since the device using cryptocommunication is omitted, it has simple structure. Since many functions (living body data-hold, the collating count section, signature processing, signature key maintenance) were given to IC card 3b, the load to IC card 3b is large. Therefore, if the IC card of the dedication limited to this application is published, more effective systems operation will become possible.
[0100] in addition, the thing obtained by making natural effectiveness corresponding to the configuration which was common by the relation between this operation gestalt and each above-mentioned operation gestalt also in this operation gestalt -- it is -- the above -- explanation is omitted here about the effectiveness explained with which operation gestalt.

[0101] (Gestalt of implementation of the 3rd of invention) Drawing 5 is the block diagram showing an example of the user check system by the living body data concerning the gestalt of operation of the 3rd of this invention, it gives the same sign to the same part as drawing 1 , omits explanation, and describes only a part different here.

[0102] This user check system is a data - sensor count mold, and is constituted from sensor module 1c, computer 2c, and IC card3c by the IC card of the candidate systems of drawing 15 . In this system, collating count is performed by the sensor module side, and living body data are held to an IC card side.
[0103] Sensor module 1c is a stand-alone type, and consists of a sensor 11, the collating count section 13, an identification character string attaching part 14, the decode processing section 21, and a decode key attaching part 22.

[0104] Moreover, IC card 3c consists of the check processing section 17, the identification character string attaching part 18, the data-processing section 19, a private key attaching part 20, and encryption living body data-hold section 12b. Here, sensor module 1c and IC card 3c have high composition of tamper-proof nature.

[0105] It is enciphered and held at encryption living body data-hold section 12b in IC card 3c so that it can decode with the decode key with which an IC card holder's living body data are stored in the decode key attaching part 22.

[0106] Moreover, the decode processing section 21 of sensor module 1c has become as [provide / for the collating count section 13 / decode with the decode key in which the encryption living body data received from IC card3c are stored by the decode key attaching part 22, and].

[0107] In addition, computer 2c is constituted like the 1st operation gestalt.

[0108] Thus, the user check system by the living body data concerning the gestalt of operation of constituted this invention operates so that it may explain below.

[0109] Taking the case of access to the virtual Mall on the Internet 4, it explains also here like the 1st operation gestalt.

[0110] Drawing 6 is the flow chart showing the example of this operation gestalt of operation.

[0111] In the user check system by the living body data of this operation gestalt shown in this drawing In a command output (ST21) and IC card insertion (ST22), and a list The processing (ST26-ST31) after somatometry by the sensor was performed (ST25) and the sensor information in a sensor module and living body data were collated is the same as that of the case (drawing 2 : ST1 - ST2 list ST3-ST9) of the 1st operation gestalt shown in drawing 2 . Therefore, processing of this part omits explanation.

[0112] The living body data is decoded with the decode key of the decode processing section 21 in sensor module 1c, and the decode key attaching part 22 (ST24), and the description of this operation gestalt is in the place with which collating count of a step ST 26 is provided while the encryption living body data held at IC card 3c are sent out to sensor module 1c from IC card3c (ST23).

[0113] The effectiveness by having considered processing systems, such as a digital signature, as such configuration actuation at the he check list is explained below.

[0114] The user check system by the living body data concerning the gestalt of operation of this invention His living body data are held to IC card 3with operation (for example, digital signature) function c which an individual owns. The enciphered living body data are sent to sensor module 1c permanently kept by the specific location, and it is made to perform collating count in the sensor module 1c concerned. It can calculate safely, without revealing living body data or using an IC card for others unjustly, since the still higher tamper-proof nature to sensor module 1c and IC card 3c was given (for example, digital signature).

[0115] Moreover, since it is enciphered and living body data are stored only in IC card 3c, while being able to reduce the leakage danger of living body data, it can put that it is also at high safety about living body data on the management range of a user hand (IC card), and can protect, and a user's feeling of resistance to storing information machines and equipment for the living body data of self can be reduced sharply.

[0116] Furthermore, the system of this operation gestalt is the good system of balance that it is easy to make also in various combination, if it takes into consideration that many biometrics sensors (palm type, a retina, etc.) cannot be mounted on an IC card from the magnitude or structure, or that a load is comparatively large for performing collating count in an IC card.

[0117] However, since it is necessary to send individual living body data to the collating count section 13 of a sensor module from an IC card each time whenever it collates, encryption processing described above for security maintenance is performed. Drawing 5 serves as a system which holds the living body data enciphered with the decode key held at the sensor side as an example which can maintain sufficient security to an IC card, though it is simple if possible. Living body data are in IC card 3c, and high security is held.

[0118] Therefore, the system of this operation gestalt is [at many and unspecified persons] simply usable in many locations (system) corresponding to available, i.e., this system, and its convenience is high. That is, since it has individual living body data in an IC card, it is suitable when using one system by many and unspecified persons. However, since it is necessary to store living body data in an IC card, the memory only for living body data is further added to the IC card made for the signature.

[0119] Structurally, since this memory and the part of signature processing can be carved, if compared with the case of the omnipotent IC card mold shown with the 2nd operation gestalt, the design change of an IC card is easy. Moreover, since collating count is performed by sensor module 1c, the load of IC card 3c is also small, and can be used as a realistic system. In addition, in order to eliminate the danger of tapping of the identification character string by the hacker, it is the same as that of the 1st operation gestalt that it is desirable to encipher an identification character string and to send to an IC card.

[0120] Moreover, although encryption living body data have sent the thing same each time as it is to the sensor module 1c side from IC card3c, higher security will be maintained if the easy structure of not receiving the completely same sensor information as registration data is established in the collating count section 13. It is because there is usually an error in information from a biometrics sensor and it is hardly possible that the data registered and the completely same data are acquired. The effectiveness that use of the invader who received registration data (living body data) by an unjust copy etc. can be eliminated is expected without barring a registered user's use by completely refusing the same data.

[0121] in addition, the thing obtained by making natural effectiveness corresponding to the configuration which was common by the relation between this operation gestalt and each above-mentioned operation gestalt also in this operation gestalt -- it is -- the above -- explanation is omitted here about the effectiveness explained with which operation gestalt.

[0122] (Gestalt of implementation of the 4th of invention) Drawing 7 is the block diagram showing an example of the user check system by the living body data concerning the gestalt of operation of the 4th of this invention, it gives the same sign to the same part as drawing 1 , omits explanation, and describes only a part different here.

[0123] This user check system is data - PC count mold, and is constituted from sensor module 1d, computer 2d, and 3d of IC cards by the IC card of the candidate systems of drawing 15 . By this system, at a sensor module side, it performs (easy scramble processing is performed), and only sensor input transmission holds living body data to 1d of IC cards, and performs collating count by computer (PC).

[0124] 3d of the IC cards itself is constituted like IC card 3c of the 3rd operation gestalt, and it consists of user check systems of this operation gestalt like sensor module 1b of the 2nd operation gestalt sensor module 1d.

[0125] Moreover, in addition to the same configuration as the 1st operation gestalt, components other than sensor 11 in sensor module 1c of the 3rd operation gestalt are prepared in computer 2d as the verification function section 23. In addition, this verification function section 23 consists of the collating count section 13, the identification character string attaching part 14, the decode processing section 21, and a decode key attaching part 22, and it is possible to also make it constitute as a DLL (dynamic link library). In addition, DLL is a called program for the first time, when a command starts.

[0126] Thus, actuation of the user check system by the living body data concerning the gestalt of operation of constituted this invention is explained.

[0127] Drawing 8 is the flow chart showing the example of this operation gestalt of operation.

[0128] it is shown in this drawing -- as -- the user check system of this operation gestalt -- processing of steps ST43-ST48 -- not sensor module 1d but computer 2d -- or if the point performed to computer 2d is removed, it will operate like the system of the 3rd operation gestalt shown in drawing 6 .

[0129] As mentioned above, the user check system by the living body data concerning the gestalt of operation of this invention Since the verification function section 23 was formed in the computer 2d interior reduction of a certain amount of leakage danger of living body data, and a list -- high him of certainty, enabling prevention of the improper use by the 3rd person, even when an acknowledgement function, i.e., an IC card, is lost or it is stolen It can realize by easy hardware and these functions can be used as an economical system with high actuality.

[0130] in addition, the thing obtained by making natural effectiveness corresponding to the configuration which was common by the relation between this operation gestalt and each above-mentioned operation gestalt also in this operation gestalt -- it is -- the above -- explanation is omitted here about the effectiveness explained with which operation gestalt.

[0131] (Gestalt of implementation of the 5th of invention) Drawing 9 is the block diagram showing an example of the user check system by the living body data concerning the gestalt of operation of the 5th of

this invention, it gives the same sign to the same part as drawing 1 , omits explanation, and describes only a part different here.

[0132] This user check system is IC card one apparatus of the candidate systems of drawing 15 , and consists of computer 2e and IC card3e.

[0133] A sensor 11, the living body data-hold section 12, the collating processing section 13, the data-processing section 19, and the private key attaching part 20 are formed in IC card3e of this operation gestalt, and each of these configurations are dedicated in 1 chip of IC also including the sensor 11. Moreover, in order that living body data may raise tamper-proof nature, it is constituted so that it cannot output outside, and each above-mentioned structure for raising tamper-proof nature is prepared in IC card3e.
 [0134] In addition, computer 2e is constituted like the 1st operation gestalt, if it removes that the candidate for access is only IC card 3e.

[0135] Thus, actuation of the user check system by the constituted living body data is the same as that of the 2nd operation gestalt, if the point which sensor 11 the very thing is prepared in IC card 2e, and somatometry is performed in IC card 2e, and does not have the migration between devices of sensor information is removed.

[0136] Since the user check system by the living body data concerning the gestalt of operation of this invention forms a sensor 11 in the IC card which has the configuration of the 2nd operation gestalt further and all the high information on secrecy nature processed inside IC card 3e as mentioned above, the effectiveness same about the part to which the configuration is common in the 2nd operation gestalt is acquired, and also the work using cryptocommunication can be made into unnecessary and simple protocol structure. Moreover, the tamper-proof nature itself can be made high.

[0137] (Gestalt of implementation of the 6th of invention) This operation gestalt is a system which checks the use authority of calculating-machine software by the personal authentication by the biometrics using living body data. This system carries out licence of software to insurance, without [without it uses the pocket object of tamper-proof nature such as an IC card, and] revealing living body data or being unjustly used for others.

[0138] Drawing 10 is the block diagram showing an example of the user check system by the living body data concerning the gestalt of operation of the 6th of this invention, it gives the same sign to the same part as drawing 1 , omits explanation, and describes only a part different here.

[0139] This user check system consists of sensor module 1f and computer 2f.

[0140] Sensor module 1f, it is constituted like the 2nd operation gestalt and has a sensor 11.

[0141] Collating count section 31a, encryption living body data-hold section 32a, and software 34for startup a, such as a screen saver, are prepared in computer 2f.

[0142] Each user's living body data beforehand enciphered by each user's log on password are held at encryption living body data-hold section 32a.

[0143] Collating count section 31a performs personal authentication by living body data and sensor measurement information, and if it can be checked with a use authority person, it will output a starting instruction to object software 34a.

[0144] Next, actuation of the user check system by the living body data concerning the gestalt of operation of this invention constituted as mentioned above is explained.

[0145] First, in case it begins to use object software 34a, log on password 33a is inputted by the user through an input unit (not shown).

[0146] Next, the encryption living body data which have the use authority of object software 34a are read from living body data-hold section 32a by collating count section 31a, and the decryption by input log on password 33a is performed.

[0147] Next, somatometry is performed in sensor module 1f, and it is transmitted to collating count section 31a the measurement result of whose is computer 2f. In addition, the easy scramble is applied to this transmit data.

[0148] In collating count section 31a, the received sensor information is collated with the decrypted living body data, and it checks whether those who are using the system have the use authority of software 34a for starting. In addition, log on password 33a, the decrypted living body data, and the received sensor information are recorded only on volatile memory, and such information disappears after session termination.

[0149] the user to whom those who are demanding software starting have just use authority by the above-mentioned collating count -- if it is checked that he is him, that will be notified to software 34for starting a by collating count section 31a. Thereby, starting processing of the software for starting is started.

[0150] As mentioned above, the user check system by the living body data concerning the gestalt of operation of this invention the user the living body data enciphered by the log on password concerned by inputting log on password 33a are decoded, and using biometrics -- him, since a check and an authority check are made The living body data enciphered with the password can keep the secret, even if it reveals independently, and they can also keep the use authority of software.

[0151] Furthermore, after a password etc. is recorded only on volatile memory and ending a session, since information disappears, password information etc. is not stolen even if the information on the non-volatile recorded on the hard disk etc. with a certain means may be read.

[0152] In addition, in the case of software use authority, it explained, but in software starting, this invention is not restricted and can make the technique of this operation gestalt apply also about starting of the computer itself, or starting of various devices with this operation gestalt.

[0153] Moreover, when a computer is started carrying out a user check and an authority check, for example using the technique of this operation gestalt, it is made to display the list of the software with which the

user has use authority, and to perform use of a squirrel and the raised software freely henceforth. If it does in this way, it is not necessary to carry out somatometry one by one at the time of software starting, and a user's burden can be mitigated.

[0154] (Gestalt of implementation of the 7th of invention) Drawing 11 is the block diagram showing an example of the user check system by the living body data concerning the gestalt of operation of the 7th of this invention, it gives the same sign to the same part as drawing 1 , omits explanation, and describes only a part different here.

[0155] This user check system consists of sensor module 1g, computer 2g, and 3g of IC cards.

[0156] Sensor module 1g, it is constituted like the 2nd operation gestalt and has a sensor 11.

[0157] Collating count section 31b and software 34for startup b are prepared in computer 2g.

[0158] Encryption living body data-hold section 32b holding the enciphered living body data, the cryptographic key attaching part 35 holding the cryptographic key for decoding this encryption living body data, and the log on password attaching part 36 holding a log on password are formed in 3g of IC cards. In addition, 3g of IC cards has high tamper-proof nature.

[0159] computer 2g collating count section 31b -- the user from the somatometry result of living body data and a sensor 11 -- he is checked and the result is notified to software 34for startup b.
[0160] Next, actuation of the user check system by the living body data concerning the gestalt of operation of this invention constituted as mentioned above is explained.

[0161] first, if 3g of IC cards is inserted, the log on password in an IC card will read by software 34for starting b -- having -- the collating count section 31 -- him -- a request of a check is made.
[0162] While living body measurement information is required of a sensor 11, encryption living body data and its cryptographic key are read from encryption living body data-hold section 32b and the cryptographic key attaching part 35 of 3g of IC cards by collating count section 31b requested from software 34for starting b.

[0163] while collating count section 31b which received such information decodes encryption living body data and taking out living body data -- a sensor 11 to living body measurement information -- reception and both -- comparison collating -- carrying out -- a user -- it checks whether you are him.
[0164] If it is checked that he is him, that will be notified to software 34for starting b, and starting of software 34for starting b will be started.

[0165] As mentioned above, the user check system by the living body data concerning the gestalt of operation of this invention the user only by inserting 3g of IC cards in computer 2g, the living body data enciphered by the cryptographic key are decoded, and using biometrics -- him, since a check and an authority check are made The living body data enciphered by the cryptographic key can keep the secret, even if it reveals independently, and they can also keep the use authority of software.

[0166] Furthermore, since information disappears after living body data etc. are recorded only on volatile memory in a computer and ending a session, such information is not stolen.

[0167] In addition, in the case of software use authority, it explained, but in software starting, this invention is not restricted and can make the technique of this operation gestalt apply also about starting of the computer itself, or starting of various devices with this operation gestalt.

[0168] Moreover, when a computer is started carrying out a user check and an authority check, for example using the technique of this operation gestalt, it is made to display the list of the software with which the user has use authority, and to perform use of a squirrel and the raised software freely henceforth. If it does in this way, it is not necessary to carry out somatometry one by one at the time of software starting, and a user's burden can be mitigated.

[0169] (Gestalt of implementation of the 8th of invention) This operation gestalt offers the user check system as a file encryption system which raised the security of cipher processing by recording living body data on the IC card which recorded the cryptographic key for file encryption.

[0170] Drawing 12 is the block diagram showing an example of the user check system by the living body data concerning the gestalt of operation of the 8th of this invention, it gives the same sign to the same part as drawing 1 , omits explanation, and describes only a part different here.

[0171] This user check system consists of sensor module 1h, computer 2h, and 3h of IC cards and the hard disk 5 as a secondary storage.

[0172] Sensor module 1h, it is constituted like the 2nd operation gestalt and has a sensor 11. In computer 2h, the encryption program 37 is [collating count section 31c and] **********. Moreover, living body data-hold section 32c, the code count section 38, and the cryptographic key attaching part 39 are formed in 3h of IC cards. Furthermore, the input file 40 used as a code or the candidate for decode and the output file 41 as a code or a decode result are formed in the hard disk 5.

[0173] collating count section 31c -- the user from living body data and sensor information -- he is checked and file encryption initiation authorization is notified to encryption program 37 list at the code count section 38.

[0174] the encryption program 37 -- an input file 40 -- reading -- the code or the information for decode -- the code count section 38 -- cooperating -- a code -- or it decodes and the result is outputted to an output file 41.

[0175] The code count section 38 is bearing a part of the code or decode processing which the encryption program 37 performs, and uses the cryptographic key of the cryptographic key attaching part 39 in the code or decode processing part which self performs.

[0176] In addition, 3h of IC cards has high tamper-proof nature.

[0177] Next, actuation of the user check system by the living body data concerning the gestalt of operation of this invention constituted as mentioned above is explained.

[0178] Drawing 13 is the flow chart showing actuation by this whole operation gestalt.

[0179] First, starting of the encryption program 37 is started (ST61). The encryption program 37 requests the check of whether a system user is him from collating count section 31c.

[0180] Next, living body data are read in 3h of inserted IC cards by collating count section 31c (ST62). In addition, it is enciphered by the approach of this operation gestalt, or the approach of the 3rd operation gestalt, and especially the living body data stored and sent out to living body data-hold section 32c although not illustrated are decrypted in collating count section 31c, and are used.

[0181] Next, somatometry by the sensor 11 is performed and sensor information is sent out to collating count section 31c (ST63). In addition, the easy scramble is applied to this transmit data.

[0182] next, collating of living body data and sensor information carries out in collating count section 31c -- having -- a system user -- a user -- the check of whether to be him is made (ST64). In addition, the decrypted living body data and the received sensor information are recorded only on volatile memory, and such information disappears after session termination.

[0183] As a result of carrying out the above-mentioned collating, if it is not him, an error message will be carried out and it will end, and if checked with him, a notice to that effect will be made by the encryption program 37 and the code count section 38 (ST65).

[0184] Starting of the encryption program 37 and the code count section 38 is completed, and encryption processing of a file is started by this (ST66).

[0185] That is, an input file 40 is read into the encryption program 37 (ST67), encryption or decryption processing is performed (ST68), the result is outputted to an output file (ST69), and a series of processings are completed.

[0186] Next, the encryption processing in a step ST 68 is explained in detail.

[0187] Drawing 14 is the flow chart showing the encryption processing in this operation gestalt.
[0188] First, in the encryption program 37, a random number is generated as a key of encryption (ST71), and the data for encryption (plaintext) read considering the random number concerned as a key are enciphered (ST72).

[0189] This random number is sent out to the code count section 38 in 3h of IC cards (ST73), and it is enciphered in this code count section 38 by the cryptographic key in the cryptographic key attaching part 39 (ST74).

[0190] The enciphered random number is sent out to the computer 2h encryption program 37 by the code count section 38 (ST75).

[0191] The received encryption random number is added as a header of the cipher which enciphered the plaintext at a step ST 72 by the encryption program 37, and one cipher is constituted as a whole (ST76). Namely, what was enciphered at a step ST 72 is used as a cipher body, and a cipher is generated by using as a header the random number enciphered at a step ST 75.

[0192] In this way, the generated cipher will be outputted to a hard disk 5.

[0193] On the other hand, processing that the above-mentioned encryption processing of the decryption processing in the step ST 68 of drawing 13 is reverse will be performed.

[0194] That is, the encryption program 37 decodes the header only for the header in the cipher for decode with the key in the cryptographic key attaching part 39 in delivery and the code count section 38 in the code count section 38 first.

[0195] In this way, the decoded information is a random number as a key used for enciphering the text of the cipher for decode.

[0196] This taken-out random number is sent out to the encryption program 37 from the code count section 38. The encryption program 37 which received this random number decodes the cipher text with a receiving random number, and takes out the plaintext of a basis.

[0197] In this way, the decoded plaintext will be outputted to a hard disk 5.

[0198] since the user check system by the living body data concerning the gestalt of operation of this invention stored the cryptographic key for living body data and random numbers in 3h of high IC cards of tamper-proof nature as mentioned above -- encryption processing that secrecy nature is very high -- certain -- a user -- him -- after checking, it can perform.

[0199] Moreover, since it was made to perform indirect encryption processing which used the random number with this operation gestalt, even if the random number differ whenever it carries out encryption processing and decode processing should be used and one random number should be decoded, the secret of next encryption processing and decode processing is kept, and the encryption system had with a positive user check and high security can be realized.

[0200] Furthermore, since the cryptographic key in 3h of IC cards used for the above-mentioned code decode processing is used only in the code count section 38 in an IC card, and it does not come out to the exterior of 3h of IC cards and this cryptographic key is stored in 3h of high IC cards of tamper-proof nature, the secrecy nature of a code can be raised more.

[0201] in addition, in the range which is not limited to the gestalt of each above-mentioned implementation, and does not deviate from the summary, many things are boiled and this invention can be deformed

[0202] Moreover, as a program (software means) which a computer (computer) can be made to execute, the technique indicated in the operation gestalt is stored in storages, such as magnetic disks (a floppy disk, hard disk, etc.), optical disks (CD-ROM, DVD, etc.), and semiconductor memory, and can be transmitted by

communication media and can also be distributed. In addition, the setting program which makes the count inside of a plane constitute the software means (for not only an executive program but a table and DS to be included) which a calculating machine is made to perform is also included in the program stored in a medium side. The computer which realizes this equipment reads the program recorded on the storage, and by the case, builds a software means by the setting program, and performs processing mentioned above by controlling actuation by this software means.

EFFECT OF THE INVENTION

[Effect of the Invention]

[0203] As a full account was given above, it can make it possible according to this invention, to be able to put that it is also at high safety about living body data on the management range of a user hand, and to be able to protect, as a result to reduce a user's feeling of resistance, and the leakage danger of living body data, and the user check system and IC card list by living body [with the high certainty of a user check] data with little troublesomeness on use can be further provided with a record medium.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] The block diagram showing an example of the user check system by the living body data concerning the gestalt of operation of the 1st of this invention.

[Drawing 2] The flow chart showing the example of this operation gestalt of operation.

[Drawing 3]The block diagram showing an example of the user check system by the living body data concerning the gestalt of operation of the 2nd of this invention.

[Drawing 4] The flow chart showing the example of this operation gestalt of operation.

[Drawing 5]The block diagram showing an example of the user check system by the living body data concerning the gestalt of operation of the 3rd of this invention.

[Drawing 6] The flow chart showing the example of an operation gestalt of operation.

[Drawing 7]The block diagram showing an example of the user check system by the living body data concerning the gestalt of operation of the 4th of this invention.

[Drawing 8] The flow chart showing the example of this operation gestalt of operation.

[Drawing 9]The block diagram showing an example of the user check system by the living body data concerning the gestalt of operation of the 5th of this invention.

[Drawing 10]The block diagram showing an example of the user check system by the living body data concerning the gestalt of operation of the 6th of this invention.

[Drawing 11]The block diagram showing an example of the user check system by the living body data concerning the gestalt of operation of the 7th of this invention.

[Drawing 12]The block diagram showing an example of the user check system by the living body data concerning the gestalt of operation of the 8th of this invention.

[Drawing 13] The flow chart showing actuation by this whole operation gestalt.

[Drawing 14] The flow chart showing the encryption processing in this operation gestalt.

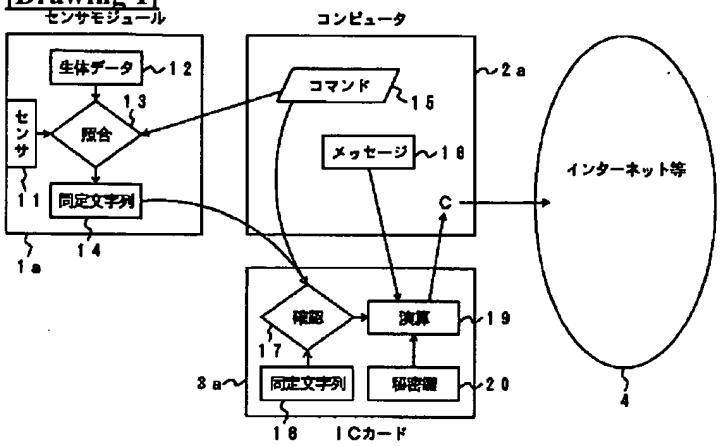
[Drawing 15] Drawing showing the component in the IC card signature system to which biometrics was made to apply, and its combination result.

[Description of Notations]

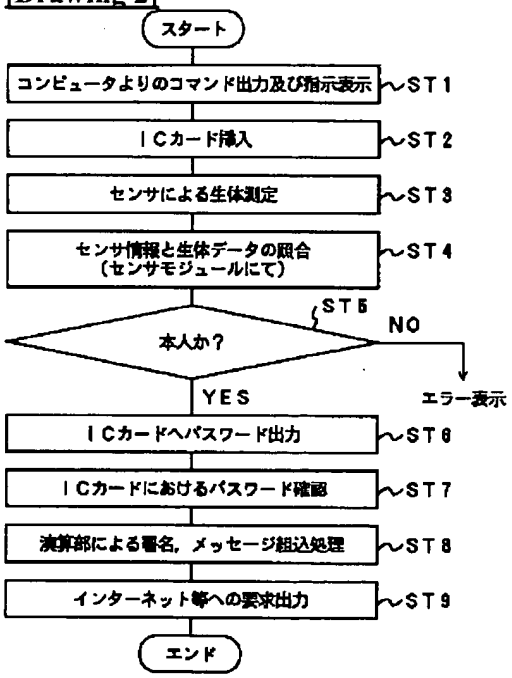
1a, 1b, 1c, 1d, 1f, 1g, 1h -- Sensor module
2a, 2b, 2c, 2d, 2e, 2f, 2g, 2h -- Computer
3a, 3b, 3c, 3d, 3e, 3g, 3h -- IC card
4 -- Internet etc.
5 -- Hard disk
11 -- Sensor
12 -- Living body data-hold section
13 -- Collating processing section
14 -- Identification character string storing section
15 -- Command output section
16 -- Message output section
17 -- Check processing section
18 -- Identification character string storing section
19 -- Data-processing section
20 -- Private key attaching part
21 -- Decode processing section
22 -- Decode key attaching part
23 -- Verification function section
31a -- Collating count section
32a -- Encryption living body data-hold section
34 -- Software for starting
37 -- Encryption program
38 -- Code count section
39 -- Cryptographic key attaching part
40 -- Input file
41 -- Output file

DRAWINGS

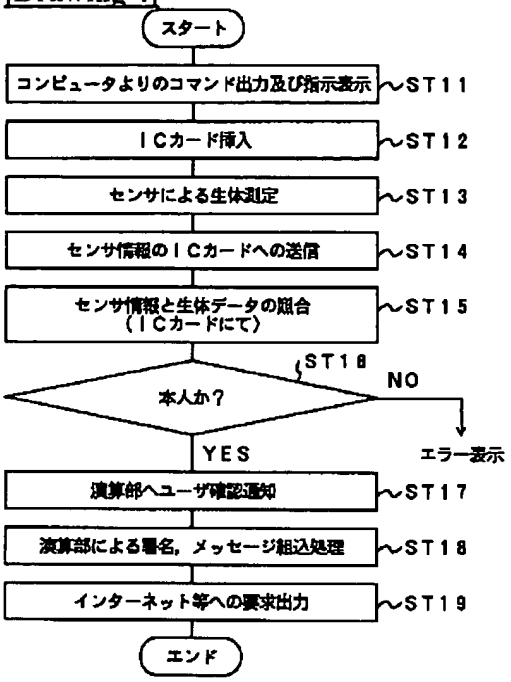
[Drawing 1]



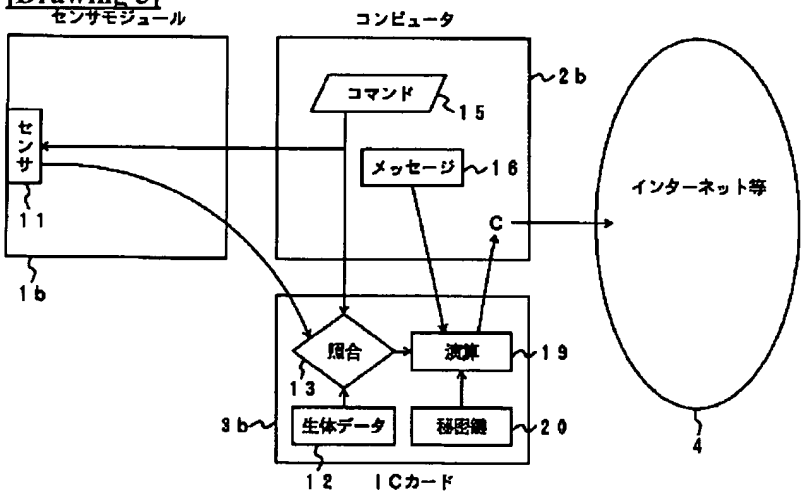
[Drawing 2]



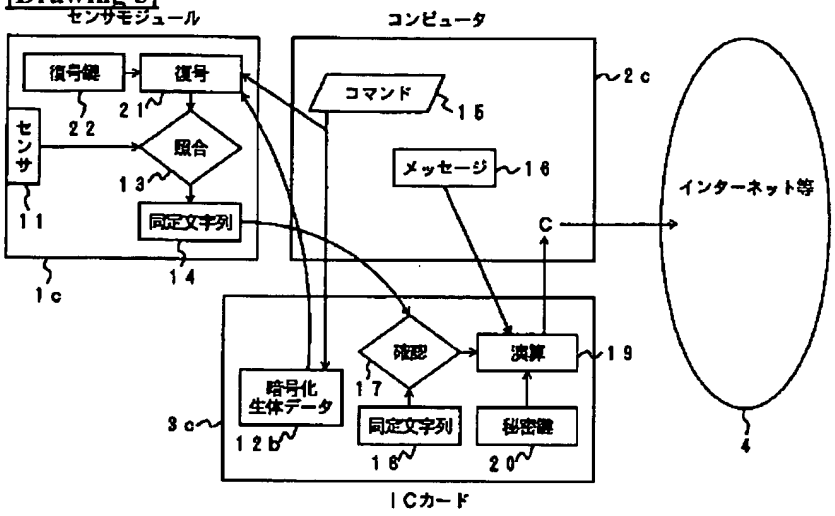
[Drawing 4]



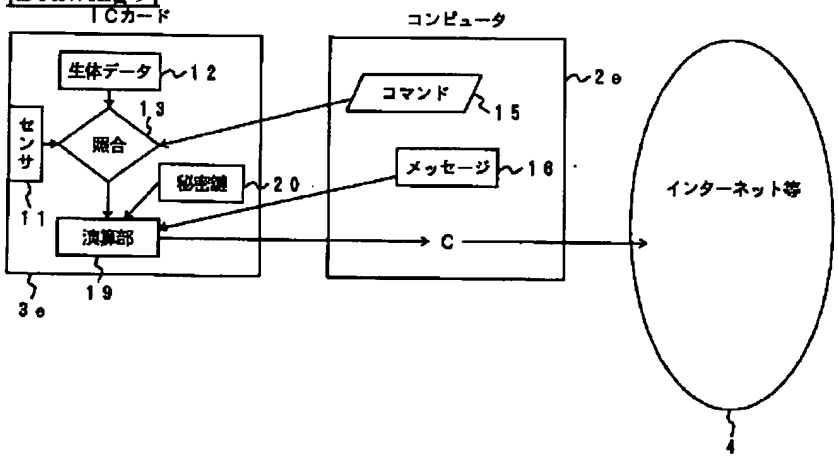
[Drawing 3]



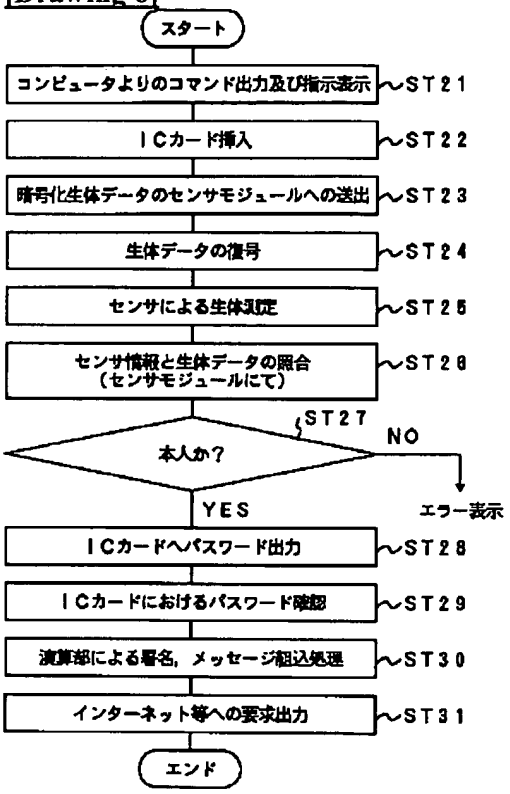
[Drawing 5]



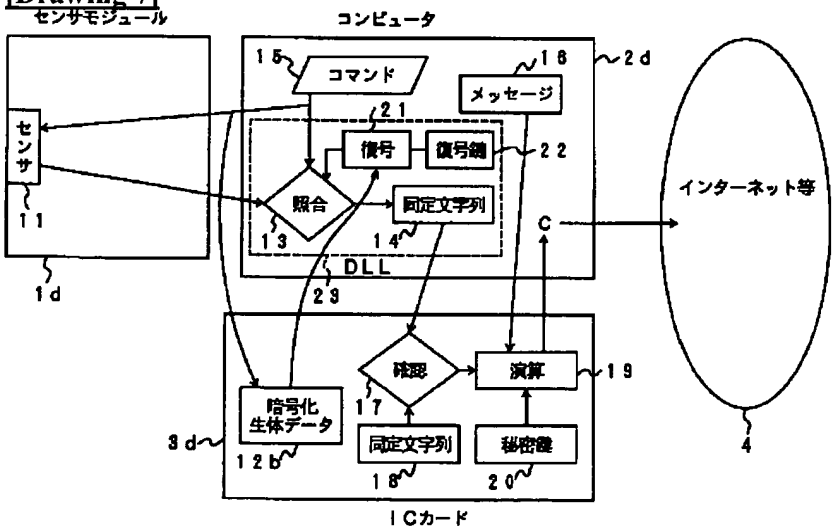
[Drawing 9]



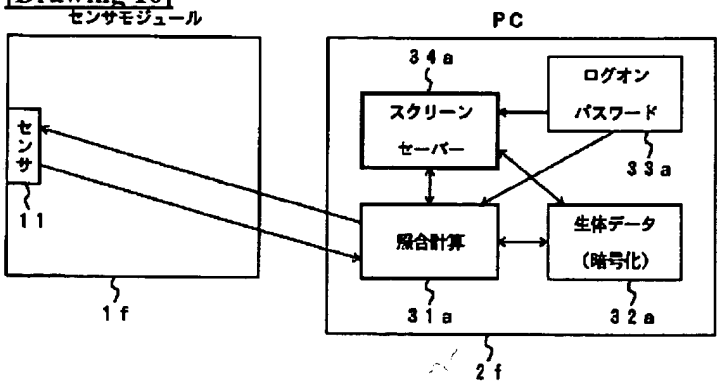
[Drawing 6]



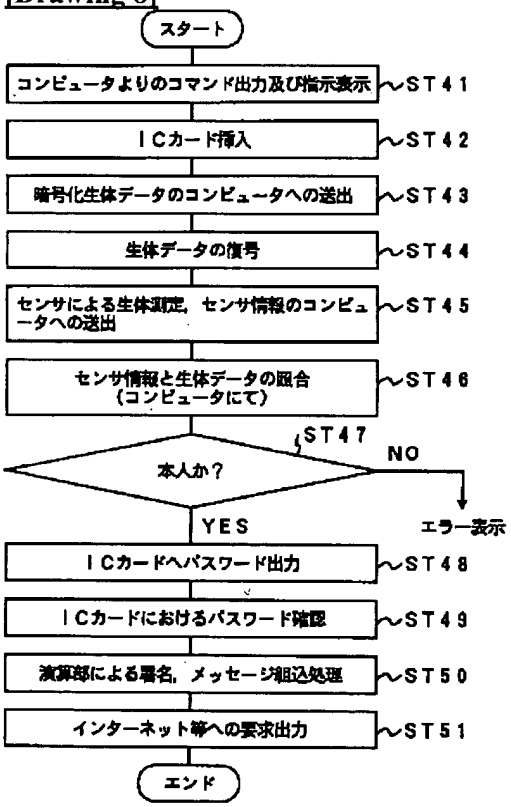
[Drawing 7]



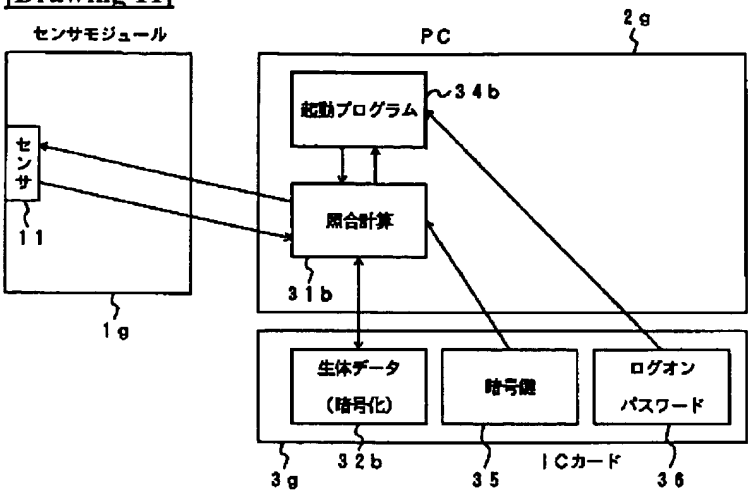
[Drawing 10]



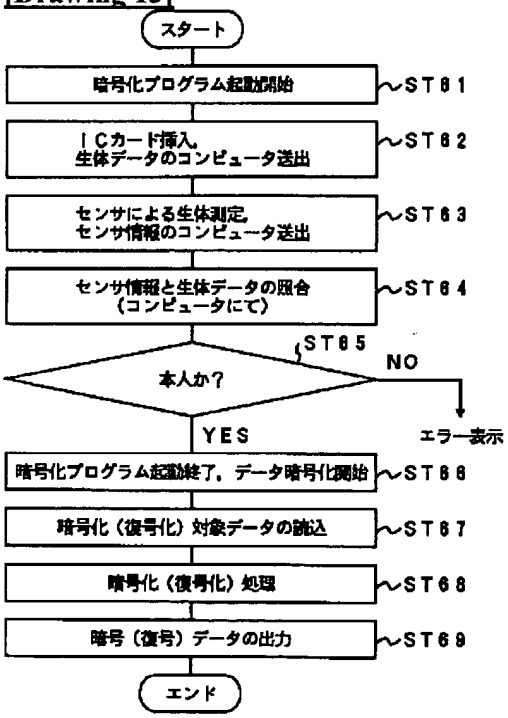
[Drawing 8]



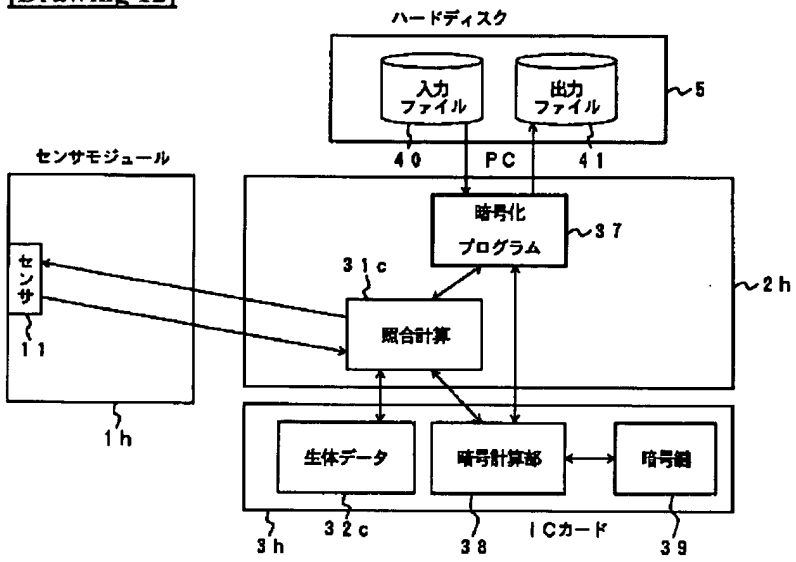
[Drawing 11]



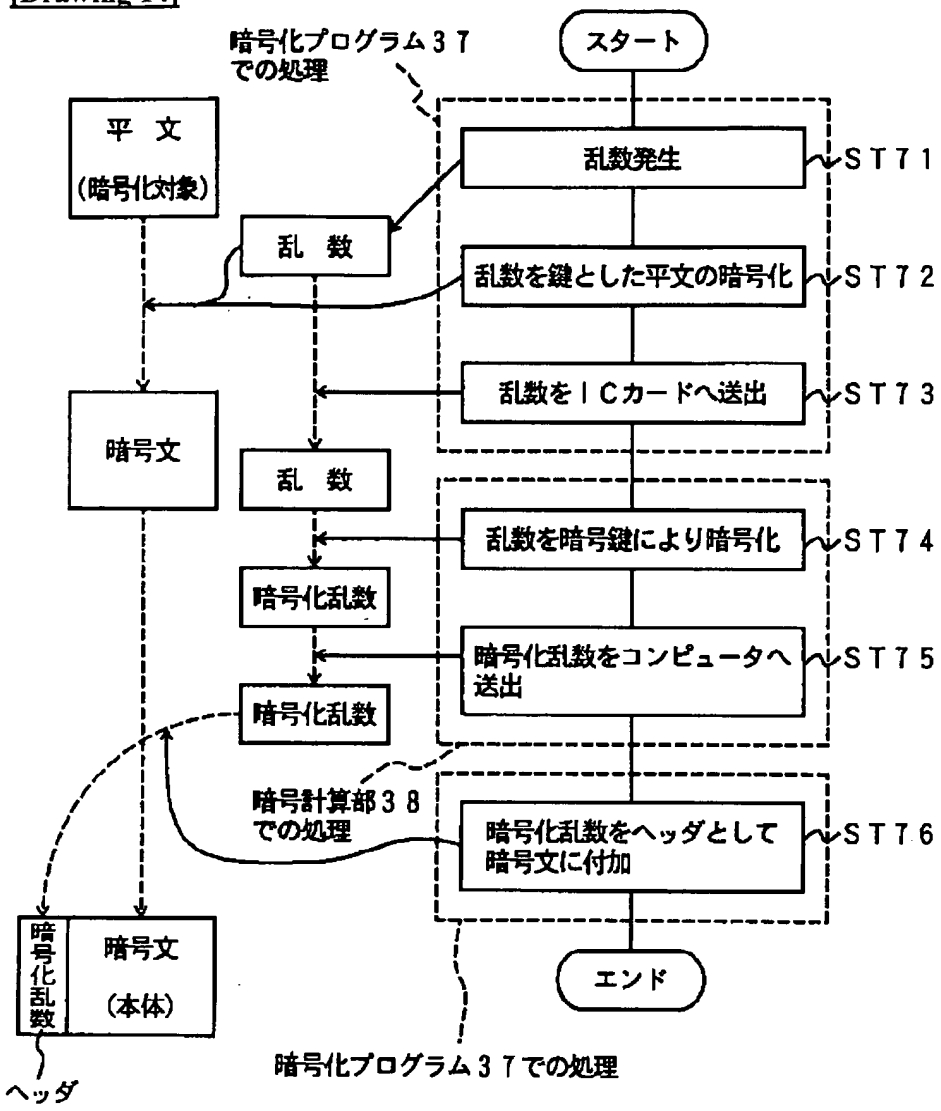
[Drawing 13]



[Drawing 12]


ハードディスク
入力ファイル
出力ファイル
5
40
PC
41
センサモジュール
暗号化プログラム
37
センサ
31c
照合計算
2h
11
1h
生体データ
暗号計算部
暗号鍵
3h
32c
38
ICカード
39

[Drawing 14]


暗号化プログラム３７での処理
スタート
平　文
（暗号化対象）
乱数発生
ＳＴ７１
乱　数
乱数を鍵とした平文の暗号化
ＳＴ７２
乱数をＩＣカードへ送出
ＳＴ７３
暗号文
乱　数
乱数を暗号鍵により暗号化
ＳＴ７４
暗号化乱数
暗号化乱数をコンピュータへ送出
ＳＴ７５
暗号化乱数
暗号計算部３８での処理
暗号化乱数をヘッダとして暗号文に付加
ＳＴ７６
暗号化乱数
暗号文
（本体）
エンド
ヘッダ
暗号化プログラム３７での処理

[Drawing 15]

	候補システム	ICカード	センサ	PC&R/W	サーバー	照合装置のタイプ	備　考
第5実施形態	ICカード一体型	生体，照合				1チップ	理想的
第1実施形態	耐タンパーモジュール一体型	PIN	PIN，生体，照合			1チップ，スタンドアロン	従来カード利用可
第2実施形態	万能ICカード型	生体，照合				従来型	準理想的
第3実施形態	ICカードにデーターセンサ計算型	生体	照合			スタンドアロン	一般的，カードに機能付加要
第4実施形態	ICカードにデーターPC計算型	生体，文字列		文字列，照合		従来型	一般的，カードに機能付加要，依頼計算の検討要
	（参考例1）	生体			照合	従来型	一般的，カードに機能付加要
	（参考例2）		生体	照合		メモリ内蔵型	変形例，従来カード利用可
	（参考例3）		生体		照合	メモリ内蔵型	変形例，従来カード利用可
	（参考例4）	照合	生体			メモリ内蔵型	変形例
	（参考例5）				生体，照合	従来型	従来カード利用可
	（参考例6）			生体（暗号化），照合		従来型	従来カード利用可

生体データと照合計算の配置可能性

[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－143833

(43)公開日　平成11年(1999)５月28日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｆ
Ｇ０９Ｃ　1/00	６６０	Ｇ０９Ｃ　1/00	６６０Ａ
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７３Ｄ

審査請求　未請求　請求項の数15　ＯＬ　（全 22 頁）

(21)出願番号　特願平9－313390

(22)出願日　平成９年(1997)11月14日

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　山田　貢己
東京都府中市東芝町１番地　株式会社東芝府中工場内

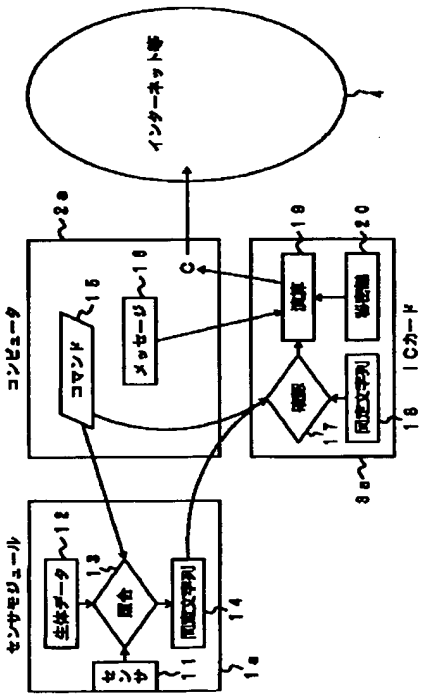
(74)代理人　弁理士　鈴江　武彦　（外６名）

(54)【発明の名称】　生体データによるユーザ確認システム及びＩＣカード並びに記録媒体

(57)【要約】

【課題】　生体データを高い安全性でもってユーザ手元の管理範囲に置いて守ることができ、ユーザの抵抗感及び生体データの漏洩危険性を低減する。

【解決手段】　生体測定を行うセンサ１１、生体データを保持する生体データ保持部１２、並びに、センサにより測定された測定情報と生体データ保持部内の生体データとを照合するとともに、照合結果より本人と確認されたときにはその旨の通知を出力する照合計算部１３を備えた耐タンパー性のセンサモジュール１ａと、通知を受けると、ユーザ確認がされたことに対応してなされるデータ出力を実行するＩＣカード３ａ，１７，１９と、センサモジュールとＩＣカードとの間の通信を行う通信手段２ａとからなる生体データによるユーザ確認システム。



1

【特許請求の範囲】

【請求項1】　生体測定を行うセンサ、生体データを保持する生体データ保持部、並びに、前記センサにより測定された測定情報と前記生体データ保持部内の生体データとを照合するとともに、照合結果より本人と確認されたときにはその旨の通知を出力する照合計算部を備えた耐タンパー性のセンサモジュールと、

前記通知を受けると、ユーザ確認がされたことに対応してなされるデータ出力を実行するＩＣカードと、

前記センサモジュールと前記ＩＣカードとの間の通信を行う通信手段とからなることを特徴とする生体データによるユーザ確認システム。

【請求項2】　生体測定を行うセンサを備えたセンサモジュールと、

生体データを保持する生体データ保持部、前記センサにより測定された測定情報と前記生体データ保持部内の生体データとを照合するとともに、照合結果より本人と確認されたときにはその旨の通知を出力する照合計算部、並びに、前記通知を受けると、ユーザ確認がされたことに対応してなされるデータ出力を実行する演算処理部を備えた耐タンパー性のＩＣカードと、

前記センサモジュールと前記ＩＣカードとの間の通信を行う通信手段とからなることを特徴とする生体データによるユーザ確認システム。

【請求項3】　生体測定を行うセンサ、暗号化された生体データを受信しこれを復号化する復号部、並びに、前記センサにより測定された測定情報と復号化された前記生体データとを照合するとともに、照合結果より本人と確認されたときにはその旨の通知を出力する照合計算部を備えたセンサモジュールと、

前記暗号化された生体データを保持するとともに、当該暗号化された生体データを前記センサモジュールに送出する生体データ保持部、並びに、前記照合計算部からの通知を受けると、ユーザ確認がされたことに対応してなされるデータ出力を実行する演算処理部を備えた耐タンパー性のＩＣカードと、

前記センサモジュールと前記ＩＣカードとの間の通信を行う通信手段とからなることを特徴とする生体データによるユーザ確認システム。

【請求項4】　前記センサモジュールに耐タンパー性を持たせたことを特徴とする請求項3記載の生体データによるユーザ確認システム。

【請求項5】　生体測定を行うセンサを備えたセンサモジュールと、

暗号化された生体データを受信しこれを復号化する復号部、並びに、前記センサにより測定された測定情報と復号化された前記生体データとを照合するとともに、照合結果より本人と確認されたときにはその旨の通知を出力する照合計算部を備えたコンピュータと、

前記暗号化された生体データを保持するとともに、当該

2

暗号化された生体データを前記コンピュータに送出する生体データ保持部、並びに、前記照合計算部からの通知を受けると、ユーザ確認がされたことに対応してなされるデータ出力を実行する演算処理部を備えた耐タンパー性のＩＣカードと、

前記センサモジュールと前記ＩＣカードと前記コンピュータとの間の通信を行う通信手段とからなることを特徴とする生体データによるユーザ確認システム。

【請求項6】　前記ＩＣカードはユーザ本人のデジタル署名を行う署名手段を備え、前記ユーザ確認がされたことに対応してなされるデータ出力には、前記署名手段によるデジタル署名が含まれることを特徴とする請求項1乃至5のうち何れか1項記載の生体データによるユーザ確認システム。

【請求項7】　生体測定を行うセンサを備えたセンサモジュールと、

ユーザ本人のログオンパスワードにより暗号化された生体データを、ユーザ要求に対応した権限を当該ユーザが有することを示す情報として保持する生体データ保持部、並びに、前記ユーザ要求及び前記ログオンパスワードが入力されたときに前記生体データ保持部の生体データを前記ログオンパスワードにより復号化するとともに、この復号化された生体データと前記センサにより測定された測定情報とを照合し、その照合結果により本人及び権限が確認されたときには、前記ユーザ要求を実施すべき旨の通知を出力する照合計算部を備えたコンピュータと、

前記コンピュータと前記センサモジュールとの間の通信を行う通信手段とからなることを特徴とする生体データによるユーザ確認システム。

【請求項8】　生体測定を行うセンサと、コンピュータと、ＩＣカードとからなり、ユーザ確認を行うとともにデータの暗号化処理を行うユーザ確認システムにおいて、

前記ＩＣカードは、耐タンパー性を有し、かつ、生体データを保持する生体データ保持部、前記データの暗号化処理におけるその一部処理を実行する第1の暗号計算部、並びに、前記第1の暗号計算部での処理に用いられる暗号鍵を保持する暗号鍵保持部を少なくとも備えており、

前記コンピュータは、ユーザ確認通知を受けると前記データの暗号化処理における他の処理を実行する第2の暗号計算部を少なくとも備えており、

さらに、前記センサにより測定された測定情報と前記生体データ保持部内の生体データとを照合するとともに、照合結果より本人と確認されたときには前記第2の暗号計算部に前記ユーザ確認通知を出力する照合計算手段と、

前記センサと前記ＩＣカードと前記コンピュータとの間の通信を行う通信手段とからなることを特徴とする生体

データによるユーザ確認システム。

【請求項9】　コンピュータに、

ユーザ本人のログオンパスワードにより暗号化された生体データを、ユーザ要求に対応した権限を当該ユーザが有することを示す情報として保持する生体データ保持機能と、

前記ユーザ要求及び前記ログオンパスワードが入力されたときに前記生体データを前記ログオンパスワードにより復号化するとともに、この復号化された生体データと生体測定された測定情報とを照合し、その照合結果により本人及び権限が確認されたときには、前記ユーザ要求を実施すべき旨の通知を出力する照合計算機能とを実現させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項10】　コンピュータに、

ユーザ確認通知を受けた場合には、データの暗号化処理における一部処理を実行するとともに、このデータ暗号化処理における他の処理の処理結果を外部から受け取り、その処理結果を前記一部処理が用いて暗号化処理を完成させる暗号計算機能と、

生体測定された測定情報とユーザ確認用の生体データとを照合するとともに、照合結果よりユーザ本人と確認されたときには前記暗号計算機能に前記ユーザ確認通知を行う照合計算機能とを実現させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項11】　暗号化された生体データを保持するとともに、この暗号化された生体データを外部装置に出力する生体データ保持手段と、

前記生体データと生体測定された測定情報とによりユーザ本人と確認された旨の照合結果を前記外部装置から通知されると、ユーザ確認がされたことに対応してなされるデータ出力を実行する演算処理手段とを備え、かつ耐タンパー性を有することを特徴とするＩＣカード。

【請求項12】　前記外部装置は、生体測定を行うセンサを有するセンサモジュールであることを特徴とする請求項11記載のＩＣカード。

【請求項13】　前記外部装置は、コンピュータであることを特徴とする請求項11記載のＩＣカード。

【請求項14】　前記演算処理手段はユーザ本人のデジタル署名を行う署名手段を備え、前記ユーザ確認がされたことに対応してなされるデータ出力には、前記署名手段によるデジタル署名が含まれることを特徴とする請求項11乃至13のうち何れか1項記載のＩＣカード。

【請求項15】　生体データを保持するとともに、この生体データを用いてユーザ確認を行う外部装置に前記生体データを出力する生体データ保持手段と、

データの暗号化処理における一部処理を暗号鍵を用いて実行するとともに、このデータの暗号化処理における他の処理を行う外部装置に前記一部処理の処理結果を出力する暗号計算手段と、

前記暗号鍵を保持する暗号鍵保持手段とを備え、かつ耐タンパー性を有することを特徴とするＩＣカード。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、ＩＣカードを利用したデジタル署名処理や、計算機ソフトウェアの使用権限確認、あるいはデータ暗号化処理の使用権限確認等を便利且つ安全に行うための生体データによるユーザ確認システム及びＩＣカード並びに記録媒体に関する。

【0002】

【従来の技術】従来からユーザを確認するのにクレジットカードや入退室管理カード等，主に磁気カードが使われている。これに対し、最近、カードの偽造や情報漏洩を防ぐ効果等を期待して、半導体チップを内蔵した高セキュリティで高機能のＩＣカードが使われ始めている。

【0003】しかしながら、ＩＣカードを利用しても、紛失や盗難により他人に不正使用されたり、紛失と偽って不正使用することに対して、それを防ぐことが難しい。

【0004】ＩＣカードに対応したパスワードを登録することにより不正使用を減らそうとすることが行われているが、パスワードは記憶することが煩わしく、忘れてしまう危険性や、メモを他人に読まれたりして漏洩する危険性があり、決して便利であるとは言えない。

【0005】最近では、指紋や掌型のような生体データを測定して本人を確認する技術であるバイオメトリクスとＩＣカードとを組み合わせて入退室管理やアクセス制御を行おうとする動きがある。これによって、カードの紛失、盗難、漏洩、忘却等により生じる各種問題は解決すると思われる。

【0006】しかし、一方でパスワードのような自由に創造できるものではなく唯一無二の自分の身体の情報（生体データ）がどこかに登録されているということに対するユーザの抵抗感や、それが漏洩したときにパスワードのような変更が効かないという弱点及び漏洩トラブルに対するユーザの不安感が根強く残っている。したがって、バイオメトリクスをユーザ確認に用いる場合には、上記抵抗感が少なくなるような技術を提案し、また、生体データの漏洩を効果的に防止できるシステムを構築する必要がある。

【0007】さらに、通常ＩＣカードを用いないことの多い計算機ソフトウェアの使用権限確認を行う環境においては、生体データを安全に保持する媒体が無く、バイオメトリクスを利用する場合には生体データを計算機の記憶媒体上に格納するしかない。しかし、この場合にはリバースエンジニアリングによって生体データが漏洩する危険性がある。

【0008】

【発明が解決しようとする課題】上述したように、従来のＩＣカードとパスワードを併用する技術では、煩わし

5

さ、忘却あるいは漏洩の危険性といった問題点がある。

【0009】また、ICカードとバイオメトリクスの併用では、自分の身体の情報（生体データ）が登録されることへの抵抗感や、生体データが第三者へ漏洩する危険性が残っている。

【0010】さらに、ICカードを用いない環境においてバイオメトリクスを利用して使用権限の確認をする場合には、生体データを安全に記録する方法が無かった。

【0011】本発明は、上記事情を考慮してなされたもので、生体データを高い安全性でもってユーザ手元の管理範囲に置いて守ることができ、ひいてはユーザの抵抗感及び生体データの漏洩危険性を低減することを可能とし、さらに使用上の煩わしさが少なくユーザ確認の確実性が高い生体データによるユーザ確認システム及びICカード並びに記録媒体を提供することを目的とする。

【0012】

【課題を解決するための手段】上記課題を解決するために、請求項1に対応する発明は、生体測定を行うセンサ、生体データを保持する生体データ保持部、並びに、センサにより測定された測定情報と生体データ保持部内の生体データとを照合するとともに、照合結果より本人と確認されたときにはその旨の通知を出力する照合計算部を備えた耐タンパー性のセンサモジュールと、通知を受けると、ユーザ確認がされたことに対応してなされるデータ出力を実行するICカードと、センサモジュールとICカードとの間の通信を行う通信手段とからなる生体データによるユーザ確認システムである。

【0013】本発明はこのような手段を設けたので、生体データ保持部内の生体データが耐タンパー性のセンサモジュールに保護され、生体データを高い安全性でもって守ることができ、生体データの漏洩危険性を低減するとともに、さらに使用上の煩わしさを少なくしユーザ本人確認の確実性を高くすることができる。

【0014】次に、請求項2に対応する発明は、生体測定を行うセンサを備えたセンサモジュールと、生体データを保持する生体データ保持部、センサにより測定された測定情報と生体データ保持部内の生体データとを照合するとともに、照合結果より本人と確認されたときにはその旨の通知を出力する照合計算部、並びに、通知を受けると、ユーザ確認がされたことに対応してなされるデータ出力を実行する演算処理部を備えた耐タンパー性のICカードと、センサモジュールとICカードとの間の通信を行う通信手段とからなる生体データによるユーザ確認システムである。

【0015】本発明はこのような手段を設けたので、請求項1に対応する発明と同様な効果が得られる他、生体データ保持部を耐タンパー性のICカードに設けたことで生体データを高い安全性でもってユーザ手元の管理範囲に置いて守ることができ、ひいてはユーザの抵抗感を低減させることができる。

6

【0016】次に、請求項3に対応する発明は、生体測定を行うセンサ、暗号化された生体データを受信しこれを復号化する復号部、並びに、センサにより測定された測定情報と復号化された生体データとを照合するとともに、照合結果より本人と確認されたときにはその旨の通知を出力する照合計算部を備えたセンサモジュールと、暗号化された生体データを保持するとともに、当該暗号化された生体データを前記センサモジュールに送出する生体データ保持部、並びに、照合計算部からの通知を受けると、ユーザ確認がされたことに対応してなされるデータ出力を実行する演算処理部を備えた耐タンパー性のICカードと、センサモジュールとICカードとの間の通信を行う通信手段とからなる生体データによるユーザ確認システムである。

【0017】本発明はこのような手段を設けたので、請求項2に対応する発明と同様な効果を得ることができる。

【0018】また、請求項4に対応する発明は、請求項3に対応する発明において、センサモジュールに耐タンパー性を持たせた生体データによるユーザ確認システムである。

【0019】本発明はこのような手段を設けたので、請求項3に対応する発明と同様な効果を得ることができる他、生体データ等の安全性を一層高めることができる。

【0020】さらに、請求項5に対応する発明は、生体測定を行うセンサを備えたセンサモジュールと、暗号化された生体データを受信しこれを復号化する復号部、並びに、センサにより測定された測定情報と復号化された生体データとを照合するとともに、照合結果より本人と確認されたときにはその旨の通知を出力する照合計算部を備えたコンピュータと、暗号化された生体データを保持するとともに、当該暗号化された生体データをコンピュータに送出する生体データ保持部、並びに、照合計算部からの通知を受けると、ユーザ確認がされたことに対応してなされるデータ出力を実行する演算処理部を備えた耐タンパー性のICカードと、センサモジュールとICカードとコンピュータとの間の通信を行う通信手段とからなる生体データによるユーザ確認システムである。

【0021】本発明はこのような手段を設けたので、請求項2に対応する発明と同様な効果をある程度は得られるとともに、簡易にかつ安価なシステムを構築することができる。

【0022】さらにまた、請求項6に対応する発明は、請求項1～5に対応する発明において、ICカードはユーザ本人のデジタル署名を行う署名手段を備え、ユーザ確認がされたことに対応してなされるデータ出力には、署名手段によるデジタル署名が含まれる生体データによるユーザ確認システムである。

【0023】本発明はこのような手段を設けたので、請求項1～5に対応する発明と同様な効果が得られる他、

ICカードを用いたデジタル署名システムを構築することができる。

【0024】一方、請求項7に対応する発明は、生体測定を行うセンサを備えたセンサモジュールと、ユーザ本人のログオンパスワードにより暗号化された生体データを、ユーザ要求に対応した権限を当該ユーザが有することを示す情報として保持する生体データ保持部、並びに、ユーザ要求及びログオンパスワードが入力されたときに生体データ保持部の生体データをログオンパスワードにより復号化するとともに、この復号化された生体データとセンサにより測定された測定情報とを照合し、その照合結果により本人及び権限が確認されたときには、ユーザ要求を実施すべき旨の通知を出力する照合計算部を備えたコンピュータと、コンピュータとセンサモジュールとの間の通信を行う通信手段とからなる生体データによるユーザ確認システムである。

【0025】本発明はこのような手段を設けたので、パスワードで暗号化された生体データはたとえ単独で漏洩してもその秘密を守ることができ、かつソフトウェアの使用権限をも守ることができる。また、バイオメトリクスを用いたユーザ本人確認及び権限確認がなされるようになっているので、使用上の煩わしさを少なくしユーザ本人確認の確実性を高くすることができる。

【0026】また、請求項8に対応する発明は、生体測定を行うセンサと、コンピュータと、ICカードとからなり、ユーザ確認を行うとともにデータの暗号化処理を行うユーザ確認システムにおいて、ICカードは、耐タンパー性を有し、かつ、生体データを保持する生体データ保持部、データの暗号化処理におけるその一部処理を実行する第1の暗号計算部、並びに、第1の暗号計算部での処理に用いられる暗号鍵を保持する暗号鍵保持部を少なくとも備えており、コンピュータは、ユーザ確認通知を受けるとデータの暗号化処理における他の処理を実行する第2の暗号計算部を少なくとも備えており、さらに、センサにより測定された測定情報と生体データ保持部内の生体データとを照合するとともに、照合結果より本人と確認されたときには第2の暗号計算部にユーザ確認通知を出力する照合計算手段と、センサとICカードとコンピュータとの間の通信を行う通信手段とからなる生体データによるユーザ確認システムである。

【0027】本発明はこのような手段を設けたので、生体データ及び暗号鍵が耐タンパー性の高いICカードに格納され、確実なユーザ本人確認がなされた後に暗号化処理を実行することができる。また、ICカードとコンピュータとで暗号化処理を分担するようにしているので、極めて秘匿性の高い暗号化を実現することができる。

【0028】さらに、請求項9に対応する発明は、コンピュータに、ユーザ本人のログオンパスワードにより暗号化された生体データを、ユーザ要求に対応した権限を当該ユーザが有することを示す情報として保持する生体データ保持機能と、ユーザ要求及びログオンパスワードが入力されたときに生体データをログオンパスワードにより復号化するとともに、この復号化された生体データと生体測定された測定情報とを照合し、その照合結果により本人及び権限が確認されたときには、ユーザ要求を実施すべき旨の通知を出力する照合計算機能とを実現させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体である。

【0029】本発明はこのような手段を設けたので、請求項7に記載した生体データによるユーザ確認システムにおけるコンピュータの動作を実現させることができる。

【0030】さらにまた、請求項10に対応する発明は、コンピュータに、ユーザ確認通知を受けた場合には、データの暗号化処理における一部処理を実行するとともに、このデータ暗号化処理における他の処理の処理結果を外部から受け取り、その処理結果を用いて暗号化処理を完成させる暗号計算機能と、生体測定された測定情報とユーザ確認用の生体データとを照合するとともに、照合結果よりユーザ本人と確認されたときには暗号計算機能にユーザ確認通知を行う照合計算機能とを実現させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体である。

【0031】本発明はこのような手段を設けたので、請求項8に記載した生体データによるユーザ確認システムにおけるコンピュータの動作を実現させることができる。

【0032】一方、請求項11に対応する発明は、暗号化された生体データを保持するとともに、この暗号化された生体データを外部装置に出力する生体データ保持手段と、生体データと生体測定された測定情報とによりユーザ本人と確認された旨の照合結果を外部装置から通知されると、ユーザ確認がされたことに対応してなされるデータ出力を実行する演算処理手段とを備え、かつ耐タンパー性を有することを特徴とするICカードである。

【0033】本発明はこのような手段を設けたので、請求項3又は5に記載した生体データによるユーザ確認システムにおけるICカードの動作を実現させることができる。

【0034】次に、請求項12に対応する発明は、請求項11に対応する発明において、外部装置は、生体測定を行うセンサを有するセンサモジュールであるICカードである。

【0035】本発明はこのような手段を設けたので、請求項3又は4に記載した生体データによるユーザ確認システムにおけるICカードの動作を実現させることができる。

【0036】また、請求項13に対応する発明は、請求項11に対応する発明において、外部装置は、コンピュ

ータであるＩＣカードである。

【００３７】本発明はこのような手段を設けたので、請求項５に記載した生体データによるユーザ確認システムにおけるＩＣカードの動作を実現させることができる。

【００３８】さらに、請求項１４に対応する発明は、請求項１１～１３に対応する発明において、演算処理手段はユーザ本人のデジタル署名を行う署名手段を備え、ユーザ確認がされたことに対応してなされるデータ出力には、署名手段によるデジタル署名が含まれるＩＣカードである。

【００３９】本発明はこのような手段を設けたので、請求項３～５に対応する発明のうち、さらに請求項６の手段も有する生体データによるユーザ確認システムにおけるＩＣカードの動作を実現させることができる。

【００４０】また、請求項１５に対応する発明は、生体データを保持するとともに、この生体データを用いてユーザ確認を行う外部装置に生体データを出力する生体データ保持手段と、データの暗号化処理における一部処理を暗号鍵を用いて実行するとともに、このデータの暗号化処理における他の処理を行う外部装置に一部処理の処理結果を出力する暗号計算手段と、暗号鍵を保持する暗号鍵保持手段とを備え、かつ耐タンパー性を有するＩＣカードである。

【００４１】本発明はこのような手段を設けたので、請求項８に記載した生体データによるユーザ確認システムにおけるＩＣカードの動作を実現させることができる。

【００４２】

【発明の実施の形態】以下、本発明の実施の形態について説明する。

【００４３】本発明は、すでに述べたように、１）生体データの漏洩危険性を低減させること、２）自己の生体データを情報機器を格納することに対するユーザの抵抗感を低減させること、を目的としており、上記１）、２）の何れか若しくは両方を実現できる手段を提供するものである。

【００４４】特に、発明者らは、生体データによるユーザ確認システムの一形態としてのＩＣカード署名システムに、バイオメトリクスを適用させる場合にいかなるシステムを構築すれば上記目的を実現できるかについて種々検討した。ここで、ＩＣカード署名システムとは、ＩＣカード内部のデジタル署名機能を作動させる機能をもったＩＣカードを利用し、そのデジタル署名により、機密情報の電子メールによる送付、インターネット上の買い物等を実現させるシステムである。このシステムにバイオメトリクスを適用させた場合には、指紋等の生体データについてのセンサ測定情報との照合結果に基づき本人確認を行い、その上でＩＣカードの上記デジタル署名機能を作動させることになる。

【００４５】発明者らは、まず、バイオメトリクスを適用させたＩＣカード署名システム（以下、単にＩＣカード署名システム又はシステムともいう）を構成し得る要素として４つのモジュール、つまりＩＣカード、センサモジュール、コンピュータ（ＰＣ、ＩＣカードリーダ／ライタ含む）、サーバーについて検討した。次に、ＩＣカード署名システムにおいて行われる処理（生体（登録）データ記録、照合計算）をそれぞれどのモジュールで行えば本発明の目的を達成できるかについて検討した。

【００４６】図１５はバイオメトリクスを適用させたＩＣカード署名システムにおける構成要素及びその組み合わせ結果を示す図である。

【００４７】図１５に示す各候補システムのうち、生体データがユーザの手元には無い中央処理装置に登録されることを嫌うユーザが存在することを考慮し、ローカルな処理によってＩＣカードの所有者確認を行うことを優先する。そのためサーバーを利用するものは、検討のこの時点では除外した。生体データをユーザ手元の管理範囲に置いて守ることができるシステムであれば、ユーザの抵抗感を低減させることができると考えられるからである。ただし、技術成果の結実である発明を解釈するに当たり、上記ユーザ抵抗感に関し特に問題がない場合には、請求項に記載された範囲内であれば、サーバー等を利用する技術も発明範囲に含まれるものである。

【００４８】次に、同一の端末（センサ、ＰＣ）を不特定多数で使用可能であること、さらに、同一人物が不特定の端末で使用可能であることの利便性を考慮し、ＩＣカードに生体データを保持するものは候補システムとして残した。

【００４９】なお、生体データ保持と照合計算部を一つの耐タンパー性のモジュール内（ＩＣカード又はセンサモジュール）においたものは候補とした残した。この場合、生体データ～照合計算部間の通信が不要となりプロトコルが単純になり、セキュリティも高くできるからである。ここで、耐タンパー性とは、内部の物や情報を原形のまま容易には外部に取り出せないような仕組みを有した性質のことである。この耐タンパー性を実現するには種々の方法が考えられるが、その方法の具体的な例については後述する。

【００５０】こうして図１５に示すように、多くの組み合わせの中から特に有効と思われる候補システムを５つ見出した。なお、同図中、「ＰＩＮ」と記したものは、ＩＣカードとＰＣ等との間で機器認証を行うための識別コードであり、署名鍵とは区別している。

【００５１】以下、図１５に示す候補システムに対応してなされた発明について第１の実施形態から第５の実施形態において説明し、さらに、同図に示さない他のシステムについて第６の実施形態から第８の実施形態において説明する。

【００５２】（発明の第１の実施の形態）図１は本発明の第１の実施の形態に係る生体データによるユーザ確認

システムの一例を示す構成図である。

【0053】このユーザ確認システムは、図15の候補システムのうちの耐タンパーモジュール一体型であり、センサモジュール1aと、コンピュータ2aと、ICカード3aとから構成されている。このシステムでは、センサモジュール1a側で生体データ保持と照合計算を行い、ICカード3a側では署名処理のみを行うセンサモジュール1aは、センサ11と、生体データ保持部12と、照合処理部13と、同定文字列格納部14とから構成されている。なお、特に図示しないが、このセンサモジュール1aには、CPU、メモリ等が内蔵され、各種情報処理が実行できるようなっている。

【0054】ここで、センサ11は、生体測定として指紋を測定し電子化情報とする手段であり、生体データ保持部12には各ユーザの生体データが格納されている。また、照合計算部13は、測定されたセンサ情報と生体データを照合し、ユーザ本人か否かを判定するとともに、ユーザ本人であった場合には、その旨の出力を通知する手段である。なお、本実施形態では、照合処理部13は、同定文字列格納部14の同定文字列（以下単にパスワードともいう）をコンピュータ2aを介してICカード3aに出力するようになっている。

【0055】ここで、センサモジュール1aは、スタンドアロン型であり、耐タンパー性を有するものである。なおスタンドアロン型とは耐タンパーセンサモジュール内に少なくともセンサ11と照合計算部13を持つものである。このシステムのセキュリティは、主にセンサモジュール1a内の生体データと照合計算部13の耐タンパー性によっている。このために、センサモジュール1aにおけるセンサ11以外の各部が1チップのICにより構成されている。また、モジュール各構成部分は強固な筐体に格納され、その蓋が開かないようになっている。さらに、強制的に蓋を開けると、生体データ保持部12、照合処理部13及び同定文字列格納部14が格納されるICチップ自体が破壊されるような仕組みになっている。本実施形態ではこの筐体を壁に埋め込んで更なる耐タンパー性を確保している。

【0056】また、センサ11以外の各部12，13，14を1チップのICで構成したこと自体が耐タンパー性を確保することにつながっている。例えばパスワード情報を磁気カードに格納した場合、磁気カードにはその磁気テープ表面に情報がそのまま保持されているので、情報保持の構造さえわかれば容易に上記パスワード情報を読み取ることができ、耐タンパー性が低い。これに対してICチップに情報を格納する場合は、そのチップ端子からコマンド等を電気信号として入力して初めて情報が端子から得られることになる。この操作を実行するのは高い技術が必要であり、その分耐タンパー性が高いと言える。

【0057】また、本実施形態の場合、生体データは同一のICチップ内でのみ使用されるため、外部出力は不要であり、耐タンパー性を高めるべく生体データの外部出力はできないように構成されている。

【0058】なお、本明細書において、耐タンパー性を有するといった場合には、上記仕組みの何れかあるいはすべてが組み合わされ、また、その他の考え得る措置が取られているものである。また、ここでは、センサモジュールの場合で説明したが、ICカード等の場合でも同様な措置により耐タンパー性を高めることができる。特に、ICカードの場合は、例えばその筐体を開くと鉄粉が配線上に飛び散り、保持情報をすべて消失させるような仕組みを設けることも可能である。

【0059】また、最低限の議論として、単に耐タンパー性があるかないかを考えるときには、例えば保護したい内容が1つのICチップ内に納められているような場合には耐タンパー性はあると言えるであろう。

【0060】次に、コンピュータ2aには、コマンド出力部15と、メッセージ出力部16とが設けられている。また、コンピュータ2aにはICカードリーダ&ライタが含まれ、この点は以下の各実施形態でも同様である。

【0061】さらにコンピュータ2aは特に図示しないが、ブラウザ等の種々のアプリケーションプログラムを実行することが可能であり、本実施形態ではインターネット4に接続されている。

【0062】インターネット4では更にバーチャルモールに接続されており、コンピュータ2aからオンラインショッピングができるようになっている。コンピュータ2aに示される符号「C」は演算（デジタル署名処理等）されたメッセージであるが、後述する本実施形態の動作例ではバーチャルモールに対する物品購入等の要求出力を示している。

【0063】ICカード3aは、確認処理部17と、同定文字列格納部18と、演算処理部19と、秘密鍵保持部20とを備えており、これら各部を実現するCPUやメモリ等の資源が1チップのICに納められたものである。

【0064】確認処理部17は、センサモジュール1aからの同定文字列をICカード内の同定文字列格納部18に格納された同定文字列（パスワード）と比較し、その確認結果を演算処理部19に通知する。つまり、センサモジュール1aとICカード3aは、本人が確認されたか否かの情報をセンサモジュールからICカードへ秘密裏に伝えるための同定文字列を共有していることになる。具体的には、ICカード側の同定文字列はセンサモジュール側の同定文字列と同一であるか、或いは、ちょうどUNIXにおける暗号化パスワードのように、センサモジュール側の同定文字列を暗号化したものでもよい。要するにセンサモジュールから送られた同定文字列に対応して唯一のICカード内同定文字列が対応するよ

うになっている。

【0065】演算処理部19は、システム使用者がユーザ本人であることの確認通知を確認処理部17から受けると、所定の演算処理を実行して、演算されたメッセージCを出力する。このメッセージは、例えば入室管理上の扉開メッセージでもよいし、また例えば計算機等の装置起動命令でもよい。ここで演算処理部19は具体的な一例として、秘密鍵保持部20に格納される秘密鍵を用いてデジタル署名を行うとともに、メッセージ出力部16の情報を元にインターネット上のバーチャルモールに物品購入要求を演算されたメッセージCとして出力する。

【0066】次に、以上のように構成された本発明の実施の形態に係る生体データによるユーザ確認システムの動作について説明する。

【0067】上記したように生体データによるユーザ確認システムは種々の場合に適用できるが、ここでは、インターネット上のバーチャルモールに物品購入要求を出力する場合を例にとってその動作例を説明する。

【0068】図2は本実施形態の動作例を示す流れ図である。

【0069】この動作例では、自宅や会社でコンピュータ2aとしてのパーソナルコンピュータ（パソコン）を立ち上げブラウザソフトを起動し、インターネット4さらにはバーチャルモールに接続して物品購入をしようとする場合を想定している。

【0070】ユーザは、バーチャルモールにおいて商品及びその購入数量を選択決定し、パソコン上の購入ボタンをクリックする。この操作により図1に示すようにコンピュータ2aからコマンド15がセンサモジュール1a及びICカード3aに出力され、各種指示等の表示がコンピュータ2a上になされる（ST1）。

【0071】ここで、ICカード3aがシステムに未挿入の場合には、コンピュータ2aから「ICカードを挿入してください」とのメッセージが出され、ユーザによりICカード3aが挿入される（ST2）。なお、カード挿入に伴いコンピュータ2aから当該カード3aに物品購入処理が開始されたことが通知（コマンド15）される。

【0072】次に、ユーザが自分の指をセンサモジュール1aのセンサ11に押し当てると、センサ11による生体測定が実行される（ST3）。

【0073】次に、測定されたセンサ情報はセンサモジュール1aの照合計算部13において生体データと照合され（ST4）、本人が確認されれば（ST5）、同定文字列格納部14内の同定文字列（パスワード）がICカード3aに出力される（ST6）。なお、この処理は、従来システムにおけるパスワードのキー入力に代わるものである。また、センサモジュール1aからICカード3aへの同定文字列送出において、ハッカーによる同定文字列の盗聴の危険性を排除するためには、同定文字列を生で送る代わりに暗号化すればよい。

【0074】また、ステップST5において、本人が確認できない場合には、システム使用者がユーザ本人でない旨が表示され、以降の処理は中止される。

【0075】ICカード3aの確認処理部17においては、受信した同定文字列がカード内の保持された同定文字列と比較され、システム使用者がユーザ本人であることが確認される（ST7）。本人確認がなされればその旨が演算処理部19に通知される。

【0076】本人確認の通知を受けた演算処理部19により、メッセージ出力部16からの物品購入情報に基づいてメッセージCが作成されるとともに、そのメッセージCには秘密鍵保持部20に保持される秘密鍵によりデジタル署名が行われる（ST8）。

【0077】こうして作成され演算されたメッセージCは、コンピュータ2aからインターネット4に出力され、バーチャルモールでの物品購入が実現されることになる。

【0078】上述したように、本発明の実施の形態に係る生体データによるユーザ確認システムは、生体データ保持部12と生体データによる照合を行う照合計算部13とを同一のセンサモジュール1a内に格納して生体データがセンサモジュール1a外に出力しないようにし、かつ、センサモジュール1a自体に高い耐タンパー性を持たせたので、生体データの漏洩危険性をほとんど無くすことができ、ひいてはこれによって自己の生体データを情報機器を格納することに対するユーザの抵抗感を低減させることができる。

【0079】また、デジタル署名等を行うに際してパスワード入力でなく、本人への生体測定に基づきユーザ確認をするようにしているので、極めて確実性の高い本人確認を行うことができる。したがって、例えばICカードが紛失したり、盗まれた場合でも第3者による悪用を防止することができる。

【0080】さらに、本システムでは、照合計算部13による照合ののち、その結果をパスワードを用いて演算処理部19に通知するようにしたので、本人を確認してからデジタル署名するまでの処理を安全に行うことができ、極めてセキュリティの高いICカード署名システムを実現することができる。したがって、例えばICカードを含めたシステム全体が盗まれるようなことがあっても、盗難者は生体データを得ることも偽のメッセージCを出力することもできない。なお、このような場合に、秘密鍵や同定文字列が漏洩しないようにICカード3a自体にも高い耐タンパー性が与えられている。

【0081】また、本実施形態のシステムではバイオメトリクスを利用しているので、パスワード等を記憶しておく必要もなく、パスワード入力の煩わしさやその忘却、漏洩の危険性のないシステムを提供することができ

る。

【0082】さらに、本実施形態では、センサ11、生体データ保持部12、照合処理部13、同定文字列格納部14、確認処理部17、同定文字列格納部18、演算処理部19及び秘密鍵保持部20の各構成要件を図1に示すようにセンサモジュール1a及びICカード3aに配置したので、上記各効果の他、ICカード利用上のメリットも得られる。つまり、従来の署名用のICカードをほとんどそのまま利用することができる。その意味で、本実施形態は既カード利用型とも言える。指紋照合処理の採用を念頭に入れた特殊なICカードを発行する必要がないため、ソフトウェアの変更だけですぐにシステムを導入できる。照合計算部13がICカード3a上にないためICカードへの負荷を小さくできる。

【0083】なお、上記動作例ではバーチャルモールでの買い物の場合で説明したが、より具体的には、例えばSET (Secure Electronic Transaction)の購入要求への導入が考えられる。SETは元来磁気カードを念頭に置いた仕様であるが、実用形態としてはICカード（＋パスワード）の使用もできる。カード会員による検証と購入要求における「会員の秘密鍵で署名」の処理に本実施形態で説明した技術を導入するとその有用性が高まると考えられる。

【0084】また、本実施形態では、生体データとして指紋を用いたが、本発明はこれに限られるものでなく、掌型や声紋、網膜、顔写真等、その他種々の生体データを用いる場合にも適用することができる。また、センサ11とICカード内のデジタル署名機能部分19，20とが分離しているので、使用するセンサ種類の自由度を大きくすることができる。

【0085】さらに、本実施形態のシステムでは、センサモジュール1aの生体データ保持部12に複数の生体データをできるようにすることで、個人用のシステムとしてだけでなく、多数人が同一システムを使用できるようにすることも可能である。

（発明の第2の実施の形態）図3は本発明の第2の実施の形態に係る生体データによるユーザ確認システムの一例を示す構成図であり、図1と同一部分には同一符号を付して説明を省略し、ここでは異なる部分についてのみ述べる。

【0086】このユーザ確認システムは、図15の候補システムのうちの万能ICカード型であり、センサモジュール1bと、コンピュータ2bと、ICカード3bとから構成されている。本システムでは、センサモジュール1bではセンサ入力情報送信のみ（簡単なスクランブル処理は行う）を行い、ICカード3b側で署名処理に加えて生体データ保持と照合計算を行う。

【0087】図3に示す各構成におけるセンサ11、生体データ保持部12、照合処理部13、確認処理部17、演算処理部19及び秘密鍵保持部20の機能は第1の実施形態の図1に示されるものと同様である。ただし、その各部の配置場所が異なっている。

【0088】すなわち、本実施形態では、センサモジュール1bにはセンサ11のみが設けられている。一方、ICカード1bには、生体データ保持部12、照合処理部13、確認処理部17、演算処理部19及び秘密鍵保持部20が設けられ、これらは同一ICチップ内に構成される。なお、コンピュータ2bの構成は第1実施形態のコンピュータ2aと同様である。

【0089】各部がこのように配置されることからセンサモジュール1bにはそれほど高い耐タンパー性は必要ないが、ICカード3bには高い耐タンパー性が要求され、第1の実施形態で説明したような手段で耐タンパー性が確保されている。

【0090】次に、以上のように構成された本発明の実施の形態に係る生体データによるユーザ確認システムの動作について説明する。

【0091】ここでも第1の実施形態と同様にインターネット4上のバーチャルモールへのアクセスを例にとって説明する。

【0092】図4は本実施形態の動作例を示す流れ図である。

【0093】同図において、ステップST11からST13までの処理は第1の実施形態の図2ステップST1からST3までと同様である。

【0094】次に、センサモジュール1bからは測定されたセンサ情報がICカード3bに送出される（ST14）。センサ情報を受け取ったICカード3bでは第1の実施形態のセンサモジュール1a内で処理と同様な照合が実行される（ST15）。なお、この照合処理はICカード3b内のみで行われるので、耐タンパー性を高めるため、生体データ保持部12の生体データはICカード3bから外部に出力できない構成となっている。

【0095】照合により本人確認がなされると（ST16）、その確認結果が演算処理部19に通知され（ST17）、以下第1実施形態と同様に、デジタル署名等行われ（ST18）、演算されたメッセージCがバーチャルモールへ出力される（ST19）。

【0096】上述したように、本発明の実施の形態に係る生体データによるユーザ確認システムは、照合処理部13と生体データ保持部12を同一のICカード3bに格納するとともに、当該カード3bの耐タンパー性を高くしたので、生体データの漏洩危険性を低減させることができるとともに、生体データを高い安全性でもってユーザ手元の管理範囲（ICカード）に置いて守ることができ、自己の生体データを情報機器を格納することに対するユーザの抵抗感を大幅に低減させることができる。つまり、個人所有するICカードにセンサ以外の主要な要素がすべて実装されているため、心理的にも安心感が強い。

【0097】また、照合計算部13と演算処理部19が同一ICチップ内に構成されるので、本人を確認してからデジタル署名するまでの処理を安全に行うことができ、極めてセキュリティの高いICカード署名システムを実現することができる。

【0098】また、本実施形態のシステムでは、センサモジュール側では比較的原始的な信号処理のみを受け持たせているので、センサモジュール1bの負担を小さくすることができる。

【0099】万能ICカード型は照合装置に対して特別な要請は無く、どの型の指紋照合装置でも適用可能である。このシステムのセキュリティはもっぱらICカードの耐タンパー性に基づいており、暗号通信を用いた工夫は行っていないためシンプルな構造となっている。ICカード3bに多くの機能（生体データ保持、照合計算部、署名処理、署名鍵保持、）を持たせたため、ICカード3bへの負荷は大きい。したがって、この用途に限定した専用のICカードを発行するとより効果的なシステム運用が可能となる。

【0100】なお、本実施形態と上記各実施形態との関係で共通した構成に対応した効果は、本実施形態においても当然にして得られるものであり、上記何れかの実施形態で説明した効果についてはここでは説明を省略する。

【0101】（発明の第3の実施の形態）図5は本発明の第3の実施の形態に係る生体データによるユーザ確認システムの一例を示す構成図であり、図1と同一部分には同一符号を付して説明を省略し、ここでは異なる部分についてのみ述べる。

【0102】このユーザ確認システムは、図15の候補システムのうちのICカードにデータ～センサ計算型であり、センサモジュール1cと、コンピュータ2cと、ICカード3cとから構成されている。本システムでは、センサモジュール側で照合計算を行い、ICカード側に生体データを保持する。

【0103】センサモジュール1cは、スタンドアロン型であり、センサ11と、照合計算部13と、同定文字列保持部14と、復号処理部21と、復号鍵保持部22とから構成されている。

【0104】また、ICカード3cは、確認処理部17と、同定文字列保持部18と、演算処理部19と、秘密鍵保持部20と、暗号化生体データ保持部12bとから構成されている。ここで、センサモジュール1c及びICカード3cは耐タンパー性の高い構成となっている。

【0105】ICカード3cにおける暗号化生体データ保持部12bには、ICカード保持者の生体データが復号鍵保持部22に格納される復号鍵で復号できるように暗号化され保持されている。

【0106】また、センサモジュール1cの復号処理部21は、ICカード3cから受け取った暗号化生体データを復号鍵保持部22に格納される復号鍵で復号して照合計算部13に提供するようなっている。

【0107】なお、コンピュータ2cは、第1の実施形態と同様に構成される。

【0108】このように構成された本発明の実施の形態に係る生体データによるユーザ確認システムは次に説明するように動作する。

【0109】ここでも第1の実施形態と同様にインターネット4上のバーチャルモールへのアクセスを例にとって説明する。

【0110】図6は本実施形態の動作例を示す流れ図である。

【0111】同図に示す本実施形態の生体データによるユーザ確認システムにおいて、コマンド出力（ST21）及びICカード挿入（ST22）、並びに、センサによる生体測定が行われ（ST25）、センサモジュールにおけるセンサ情報と生体データの照合された以降の処理（ST26～ST31）は、図2に示す第1の実施形態の場合（図2：ST1～ST2並びにST3～ST9）と同様である。したがって、この部分の処理は説明を省略する。

【0112】本実施形態の特徴は、ICカード3cに保持された暗号化生体データがICカード3cからセンサモジュール1cに送出されるとともに（ST23）、その生体データがセンサモジュール1c内の復号処理部21及び復号鍵保持部22の復号鍵により復号され（ST24）、ステップST26の照合計算に提供されるところにある。

【0113】本人確認並びにデジタル署名等の処理体系をこのような構成動作としたことによる効果について以下に説明する。

【0114】本発明の実施の形態に係る生体データによるユーザ確認システムは、個人が所有する演算（例えばデジタル署名）機能付きICカード3cに本人の生体データを保持し、暗号化された生体データを特定の場所に常置されたセンサモジュール1cに送って当該センサモジュール1cにて照合計算を行うようにし、さらにセンサモジュール1c及びICカード3cに高い耐タンパー性を持たせたので、生体データが漏洩したりICカードが他人に不正に使用されたりすることなく、安全に演算（例えばデジタル署名）を行うことができる。

【0115】また、生体データは暗号化されてICカード3cのみに格納されているので、生体データの漏洩危険性を低減させることができるとともに、生体データを高い安全性でもってユーザ手元の管理範囲（ICカード）に置いて守ることができ、自己の生体データを情報機器を格納することに対するユーザの抵抗感を大幅に低減させることができる。

【0116】さらに、本実施形態のシステムは、多くのバイオメトリクスセンサ（掌型、網膜など）はその大き

さや仕組みからＩＣカード上に実装できないことや、照合計算をＩＣカードの中で行うには比較的負荷が大きいことを考え合わせると、様々な組み合わせの中でも作り易くバランスの良いシステムとなっている。

【０１１７】しかしながら、照合を行う度に毎回ＩＣカードから個人の生体データをセンサモジュールの照合計算部１３へ送る必要があるため、セキュリティ保持のために上記した暗号化処理が行われている。図5は、なるべく簡素でありながら十分なセキュリティを保つことのできる例として、センサ側に保持された復号鍵によって暗号化された生体データをＩＣカードに保持するシステムとなっている。ＩＣカード３ｃに生体データがあり、高いセキュリティが保持される。

【０１１８】したがって、本実施形態のシステムは、不特定多数で簡単に利用可能、つまり本システムに対応した多くの場所（システム）で使用可能であり利便性が高い。すなわち、ＩＣカードに個人の生体データを持つため、一つのシステムを不特定多数で使う場合に適している。ただし、ＩＣカードに生体データを格納する必要があるため、署名用に作られたＩＣカードにさらに生体データ専用のメモリが追加されている。

【０１１９】構造的にはこのメモリと署名処理の部分は切り分けられるため、第2の実施形態で示した万能ＩＣカード型の場合に比べればＩＣカードの設計変更は容易である。また、照合計算をセンサモジュール１ｃで行うのでＩＣカード３ｃの負荷も小さく、現実的なシステムとすることができる。なお、ハッカーによる同定文字列の盗聴の危険性を排除するためには同定文字列を暗号化してＩＣカードに送るのが好ましいことは第1の実施形態と同様である。

【０１２０】また、暗号化生体データは毎回そのまま同じものをＩＣカード３ｃからセンサモジュール１ｃ側に送っているが、登録データと全く同一のセンサ情報は受け付けないという簡単な仕組みを照合計算部１３内に設けると、より高いセキュリティが保たれる。というのは通常バイオメトリクスセンサからの情報には誤差があり、登録されているデータと全く同一のデータが取得されることは殆ど有り得ないからである。全く同一のデータを拒否することにより正規ユーザの使用を妨げること無く、不正なコピーなどによって登録データ（生体データ）を入手した侵入者の使用を排除できるという効果が期待される。

【０１２１】なお、本実施形態と上記各実施形態との関係で共通した構成に対応した効果は、本実施形態においても当然にして得られるものであり、上記何れかの実施形態で説明した効果についてはここでは説明を省略する。

【０１２２】（発明の第４の実施の形態）図7は本発明の第４の実施の形態に係る生体データによるユーザ確認システムの一例を示す構成図であり、図１と同一部分には同一符号を付して説明を省略し、ここでは異なる部分についてのみ述べる。

【０１２３】このユーザ確認システムは、図１５の候補システムのうちのＩＣカードにデータ～ＰＣ計算型であり、センサモジュール１ｄと、コンピュータ２ｄと、ＩＣカード３ｄとから構成されている。このシステムでは、センサモジュール側ではセンサ入力情報送信のみ（簡単なスクランブル処理は行う）を行い、ＩＣカード１ｄに生体データを保持し、コンピュータ（ＰＣ）で照合計算を行う。

【０１２４】本実施形態のユーザ確認システムでは、ＩＣカード３ｄ自体は、第３の実施形態のＩＣカード３ｃと同様に構成され、センサモジュール１ｄは、第2の実施形態のセンサモジュール１ｂと同様に構成されている。

【０１２５】また、コンピュータ２ｄには、第1の実施形態と同様な構成に加え、第３の実施形態のセンサモジュール１ｃにおけるセンサ１１以外の構成部分が照合機能部２３として設けられている。なお、この照合機能部２３は、照合計算部１３と、同定文字列保持部１４と、復号処理部２１と、復号鍵保持部２２とからなっており、ＤＬＬ（ダイナミック　リンク　ライブラリ）として構成させることも可能である。なお、ＤＬＬは、コマンドがスタートしたときに初めて呼ばれるプログラムである。

【０１２６】このように構成された本発明の実施の形態に係る生体データによるユーザ確認システムの動作について説明する。

【０１２７】図8は本実施形態の動作例を示す流れ図である。

【０１２８】同図に示すように、本実施形態のユーザ確認システムは、ステップＳＴ４３～ＳＴ４８の処理がセンサモジュール１ｄでなくコンピュータ２ｄにより若しくはコンピュータ２ｄに対して行われる点を除けば、図６に示す第３の実施形態のシステムと同様に動作する。

【０１２９】上述したように、本発明の実施の形態に係る生体データによるユーザ確認システムは、コンピュータ２ｄの内部に照合機能部２３を設けるようにしたので、ある程度の生体データの漏洩危険性の低減、並びに、確実性の高い本人確認機能，すなわちＩＣカードが紛失したり、盗まれた場合でも第３者による悪用の防止を可能としつつ、これらの機能を簡単なハードウエアで実現し経済的でかつ現実性の高いシステムとすることができる。

【０１３０】なお、本実施形態と上記各実施形態との関係で共通した構成に対応した効果は、本実施形態においても当然にして得られるものであり、上記何れかの実施形態で説明した効果についてはここでは説明を省略する。

【０１３１】（発明の第５の実施の形態）図9は本発明

の第５の実施の形態に係る生体データによるユーザ確認システムの一例を示す構成図であり、図１と同一部分には同一符号を付して説明を省略し、ここでは異なる部分についてのみ述べる。

【０１３２】このユーザ確認システムは、図１５の候補システムのうちのＩＣカード一体型であり、コンピュータ２ｅと、ＩＣカード３ｅとから構成されている。

【０１３３】本実施形態のＩＣカード３ｅには、センサ１１、生体データ保持部１２、照合処理部１３、演算処理部１９及び秘密鍵保持部２０が設けられており、これらの各構成がセンサ１１も含めてＩＣの１チップ内に納められている。また、生体データは耐タンパー性を高めるために外部に出力できないように構成されており、ＩＣカード３ｅには、耐タンパー性を高めるための上記各仕組みが設けられている。

【０１３４】なお、コンピュータ２ｅは、アクセス対象がＩＣカード３ｅのみであることを除けば第１の実施形態と同様に構成されている。

【０１３５】このように構成された生体データによるユーザ確認システムの動作は、センサ１１自体がＩＣカード２ｅ内に設けられ、ＩＣカード２ｅにて生体測定が行われセンサ情報の機器間移動がない点を除けば、第２の実施形態と同様である。

【０１３６】上述したように、本発明の実施の形態に係る生体データによるユーザ確認システムは、第２の実施形態の構成を有するＩＣカードにさらにセンサ１１を設けて秘匿性の高い情報は全てＩＣカード３ｅの内部で処理するようにしたので、第２の実施形態とその構成が共通する部分について同様な効果が得られる他、暗号通信を用いた工夫は不要でありシンプルなプロトコル構造とすることができる。また、耐タンパー性自体も高いものとすることができる。

【０１３７】（発明の第６の実施の形態）本実施形態は、計算機ソフトウェアの使用権限を、生体データを利用したバイオメトリクスによる個人認証で確認するシステムである。本システムは、ＩＣカード等の耐タンパー性の携帯物を使用することなく、また、生体データが漏洩したり他人に不正に使用されたりすることなく、ソフトウエアの使用許可を安全に行うものである。

【０１３８】図１０は本発明の第６の実施の形態に係る生体データによるユーザ確認システムの一例を示す構成図であり、図１と同一部分には同一符号を付して説明を省略し、ここでは異なる部分についてのみ述べる。

【０１３９】このユーザ確認システムは、センサモジュール１ｆとコンピュータ２ｆとから構成されている。

【０１４０】センサモジュール１ｆは、第２実施形態と同様に構成されており、センサ１１を備えたものである。

【０１４１】コンピュータ２ｆには、照合計算部３１ａと、暗号化生体データ保持部３２ａと、スクリーンセーバー等の起動対象ソフトウエア３４ａが設けられている。

【０１４２】暗号化生体データ保持部３２ａには、各ユーザのログオンパスワードで予め暗号化された各ユーザの生体データが保持されている。

【０１４３】照合計算部３１ａは、生体データとセンサ測定情報により個人認証を行い、使用権限者と確認できれば対象ソフトウェア３４ａに起動命令を出力する。

【０１４４】次に、以上のように構成された本発明の実施の形態に係る生体データによるユーザ確認システムの動作について説明する。

【０１４５】まず、対象ソフトウェア３４ａを使い始める際に、ユーザにより入力装置（図示せず）を介してログオンパスワード３３ａが入力される。

【０１４６】次に照合計算部３１ａにより、対象ソフトウエア３４ａの使用権限を有する暗号化生体データが生体データ保持部３２ａから読み出され、入力ログオンパスワード３３ａによる復号化が行われる。

【０１４７】次に、センサモジュール１ｆにおいて生体測定が行われ、その測定結果がコンピュータ２ｆの照合計算部３１ａに送信される。なお、この送信データには簡単なスクランブルがかけられている。

【０１４８】照合計算部３１ａでは、復号化された生体データと、受信したセンサ情報を照合し、システムを使用している者が起動対象のソフトウエア３４ａの使用権限を有するか否かを確認する。なお、ログオンパスワード３３ａ、復号化された生体データ及び受信したセンサ情報は揮発性メモリ上にのみ記録され、セッション終了後はこれらの情報は消えるようになっている。

【０１４９】上記照合計算により、ソフトウエア起動の要求をしている者が正当な使用権限を有するユーザ本人であると確認されると、照合計算部３１ａによりその旨が起動対象ソフトウエア３４ａに通知される。これにより、起動対象ソフトウエアの起動処理が開始される。

【０１５０】上述したように、本発明の実施の形態に係る生体データによるユーザ確認システムは、ログオンパスワード３３ａを入力することにより、当該ログオンパスワードで暗号化された生体データが復号され、バイオメトリクスを用いたユーザ本人確認及び権限確認がなされるようになっているので、パスワードで暗号化された生体データはたとえ単独で漏洩してもその秘密を守ることができ、かつソフトウェアの使用権限をも守ることができる。

【０１５１】さらに、パスワード等は揮発性メモリ上にのみ記録され、セッションを終了すると情報は消え去るため、何らかの手段でハードディスク等に記録された不揮発性の情報を読まれることがあってもパスワード情報等が盗まれることはない。

【０１５２】なお、本実施形態では、ソフトウエア使用権限の場合で説明したが、本発明はソフトウエア起動の

場合に限られるものでなく、例えば計算機自体の起動や各種機器の起動についても本実施形態の技術を適用させることができる。

【0153】また、例えば本実施形態の技術を用いてユーザ確認及び権限確認をしつつ計算機の起動をした場合に、そのユーザが使用権限を有するソフトウエアのリストを表示し、以降、リストとアップされたソフトウエアの使用は自由にできるようにしてもよい。このようにすれば、ソフトウエア起動時に一々生体測定をする必要がなく、ユーザの負担を軽減することができる。

【0154】（発明の第7の実施の形態）図11は本発明の第7の実施の形態に係る生体データによるユーザ確認システムの一例を示す構成図であり、図1と同一部分には同一符号を付して説明を省略し、ここでは異なる部分についてのみ述べる。

【0155】このユーザ確認システムは、センサモジュール1gとコンピュータ2gとICカード3gとから構成されている。

【0156】センサモジュール1gは、第2実施形態と同様に構成されており、センサ11を備えたものである。

【0157】コンピュータ2gには、照合計算部31bと、起動対象ソフトウエア34bとが設けられている。

【0158】ICカード3gには、暗号化された生体データを保持する暗号化生体データ保持部32bと、この暗号化生体データを復号するための暗号鍵を保持する暗号鍵保持部35と、ログオンパスワードを保持するログオンパスワード保持部36とが設けられている。なお、ICカード3gは高い耐タンパー性を有するものである。

【0159】コンピュータ2gの照合計算部31bは、生体データ及びセンサ11の生体測定結果からユーザ本人を確認し、その結果を起動対象ソフトウエア34bに通知する。

【0160】次に、以上のように構成された本発明の実施の形態に係る生体データによるユーザ確認システムの動作について説明する。

【0161】まず、ICカード3gが挿入されると、起動対象ソフトウエア34bによりICカード内のログオンパスワードが読み取られ、照合計算部31に本人確認の依頼がなされる。

【0162】起動対象ソフトウエア34bに依頼された照合計算部31bによって、生体測定情報がセンサ11に要求されるとともに、ICカード3gの暗号化生体データ保持部32b及び暗号鍵保持部35から暗号化生体データ及びその暗号鍵が読み出される。

【0163】これらの情報を受け取った照合計算部31bは暗号化生体データを復号して生体データを取り出すとともに、センサ11から生体測定情報を受け取り、両者を比較照合してユーザ本人か否か確認する。

【0164】本人であることが確認されればその旨が起動対象ソフトウエア34bに通知され、起動対象ソフトウエア34bの起動が開始される。

【0165】上述したように、本発明の実施の形態に係る生体データによるユーザ確認システムは、ICカード3gをコンピュータ2gに挿入するだけで、暗号鍵で暗号化された生体データが復号され、バイオメトリクスを用いたユーザ本人確認及び権限確認がなされるようになっているので、暗号鍵で暗号化された生体データはたとえ単独で漏洩してもその秘密を守ることができ、かつソフトウェアの使用権限をも守ることができる。

【0166】さらに、コンピュータにおいて生体データ等は揮発性メモリ上にのみ記録され、セッションを終了すると情報は消え去るため、これらの情報が盗まれることはない。

【0167】なお、本実施形態では、ソフトウエア使用権限の場合で説明したが、本発明はソフトウエア起動の場合に限られるものでなく、例えば計算機自体の起動や各種機器の起動についても本実施形態の技術を適用させることができる。

【0168】また、例えば本実施形態の技術を用いてユーザ確認及び権限確認をしつつ計算機の起動をした場合に、そのユーザが使用権限を有するソフトウエアのリストを表示し、以降、リストとアップされたソフトウエアの使用は自由にできるようにしてもよい。このようにすれば、ソフトウエア起動時に一々生体測定をする必要がなく、ユーザの負担を軽減することができる。

【0169】（発明の第8の実施の形態）本実施形態は、ファイル暗号化用の暗号鍵を記録したICカードに生体データも記録することにより、暗号処理のセキュリティを高めたファイル暗号化システムとしてのユーザ確認システムを提供するものである。

【0170】図12は本発明の第8の実施の形態に係る生体データによるユーザ確認システムの一例を示す構成図であり、図1と同一部分には同一符号を付して説明を省略し、ここでは異なる部分についてのみ述べる。

【0171】このユーザ確認システムは、センサモジュール1hとコンピュータ2hとICカード3hと二次記憶装置としてのハードディスク5とから構成されている。

【0172】センサモジュール1hは、第2実施形態と同様に構成されており、センサ11を備えたものである。コンピュータ2hには、照合計算部31cと、暗号化プログラム37が設られている。また、ICカード3hには、生体データ保持部32cと、暗号計算部38と、暗号鍵保持部39とが設けられている。さらに、ハードディスク5には、暗号若しくは復号対象となる入力ファイル40と、暗号若しくは復号結果としての出力ファイル41とが設けられている。

【0173】照合計算部31cは、生体データとセンサ

情報とからユーザ本人を確認し、暗号化プログラム37並びに暗号計算部38にファイル暗号化開始許可の通知をするようになっている。

【0174】暗号化プログラム37は、入力ファイル40を読み込み、その暗号若しくは復号対象情報を暗号計算部38と協力して暗号若しくは復号し、その結果を出力ファイル41に出力する。

【0175】暗号計算部38は、暗号化プログラム37が行う暗号若しくは復号処理の一部を担っており、自身が行うその暗号若しくは復号処理部分において暗号鍵保持部39の暗号鍵を使用する。

【0176】なお、ICカード3hは高い耐タンパー性を有するものである。

【0177】次に、以上のように構成された本発明の実施の形態に係る生体データによるユーザ確認システムの動作について説明する。

【0178】図13は本実施形態の全体動作を示す流れ図である。

【0179】まず、暗号化プログラム37の起動を開始する（ST61）。暗号化プログラム37は照合計算部31cにシステム使用者が本人であるか否かの確認を依頼する。

【0180】次に挿入されたICカード3hから生体データが照合計算部31cに読み取られる（ST62）。なお、特に図示しないが生体データ保持部32cに格納され送出される生体データは、本実施形態の方法あるいは第3の実施形態の方法等で暗号化されたものであり、照合計算部31cにおいて復号化されて用いられる。

【0181】次に、センサ11による生体測定が行われ、センサ情報が照合計算部31cに送出される（ST63）。なお、この送信データには簡単なスクランブルがかけられている。

【0182】次に、照合計算部31cにて生体データとセンサ情報の照合が行われ、システム使用者がユーザ本人であるか否かの確認がなされる（ST64）。なお、復号化された生体データ及び受信したセンサ情報は揮発性メモリ上にのみ記録され、セッション終了後はこれらの情報は消えるようになっている。

【0183】上記照合をした結果、本人でなければエラー表示して終了し、本人と確認されれば、その旨の通知が暗号化プログラム37及び暗号計算部38になされる（ST65）。

【0184】これによって、暗号化プログラム37及び暗号計算部38の起動が終了し、ファイルの暗号化処理が開始される（ST66）。

【0185】すなわち入力ファイル40が暗号化プログラム37に読み込まれ（ST67）、暗号化若しくは復号化処理が実行されて（ST68）、その結果が出力ファイルに出力され（ST69）、一連の処理が終了する。

【0186】次に、ステップST68における暗号化処理について詳しく説明する。

【0187】図14は本実施形態における暗号化処理を示す流れ図である。

【0188】まず、暗号化プログラム37において、暗号化の鍵として乱数が発生され（ST71）、当該乱数を鍵として読み込まれた暗号化対象データ（平文）が暗号化される（ST72）。

【0189】この乱数はICカード3h内の暗号計算部38に送出され（ST73）、この暗号計算部38において暗号鍵保持部39内の暗号鍵により暗号化される（ST74）。

【0190】暗号化した乱数は暗号計算部38によってコンピュータ2hの暗号化プログラム37に送出される（ST75）。

【0191】受信された暗号化乱数は、暗号化プログラム37によってステップST72で平文を暗号化した暗号文のヘッダとして付加され、全体として一つの暗号文が構成される（ST76）。すなわち、ステップST72で暗号化されたものを暗号文本体とし、ステップST75で暗号化された乱数をヘッダとして暗号文を生成する。

【0192】こうして生成された暗号文がハードディスク5に出力されることになる。

【0193】一方、図13のステップST68における復号化処理は上記暗号化処理の逆の処理が行われることになる。

【0194】すなわちまず、暗号化プログラム37は、復号対象の暗号文におけるヘッダのみを暗号計算部38に送り、暗号計算部38ではそのヘッダを暗号鍵保持部39内の鍵で復号する。

【0195】こうして復号された情報は、復号対象の暗号文の本文を暗号化するのに用いた鍵としての乱数である。

【0196】この取り出された乱数が暗号計算部38から暗号化プログラム37に送出される。この乱数を受信した暗号化プログラム37は、受信乱数により暗号文本文を復号し、もとの平文を取り出す。

【0197】こうして復号された平文がハードディスク5に出力されることになる。

【0198】上述したように、本発明の実施の形態に係る生体データによるユーザ確認システムは、生体データ及び乱数用の暗号鍵を耐タンパー性の高いICカード3hに格納するようにしたので、極めて秘匿性の高い暗号化処理を確実にユーザ本人確認してから実行することができる。

【0199】また、本実施形態では乱数を用いた間接的な暗号化処理を行うようにしたので、暗号化処理と復号処理を行うたびに異なる乱数が使われ、万一1個の乱数が解読されても、次回の暗号化処理と復号処理の秘密は

守られ、確実なユーザ確認と高セキュリティと兼ね備えた暗号化システムを実現することができる。

【0200】さらに、上記暗号復号処理に使用されるICカード3h内の暗号鍵はICカード内の暗号計算部38でのみ使われ、ICカード3hの外部には出ることはなく、かつ、この暗号鍵は耐タンパー性の高いICカード3h内に格納されているので、暗号の秘匿性をより高めることができる。

【0201】なお、本発明は、上記各実施の形態に限定されるものでなく、その要旨を逸脱しない範囲で種々に変形することが可能である。

【0202】また、実施形態に記載した手法は、計算機（コンピュータ）に実行させることができるプログラム（ソフトウエア手段）として、例えば磁気ディスク（フロッピーディスク、ハードディスク等）、光ディスク（CD－ROM、DVD等）、半導体メモリ等の記憶媒体に格納し、また通信媒体により伝送して頒布することもできる。なお、媒体側に格納されるプログラムには、計算機に実行させるソフトウエア手段（実行プログラムのみならずテーブルやデータ構造も含む）を計算機内に構成させる設定プログラムをも含むものである。本装置を実現する計算機は、記憶媒体に記録されたプログラムを読み込み、また場合により設定プログラムによりソフトウエア手段を構築し、このソフトウエア手段によって動作が制御されることにより上述した処理を実行する。

【0203】

【発明の効果】以上詳記したように本発明によれば、生体データを高い安全性でもってユーザ手元の管理範囲に置いて守ることができ、ひいてはユーザの抵抗感及び生体データの漏洩危険性を低減することを可能とし、さらに使用上の煩わしさが少なくユーザ確認の確実性が高い生体データによるユーザ確認システム及びICカード並びに記録媒体を提供することができる。

【図面の簡単な説明】

【図1】本発明の第1の実施の形態に係る生体データによるユーザ確認システムの一例を示す構成図。

【図2】同実施形態の動作例を示す流れ図。

【図3】本発明の第2の実施の形態に係る生体データによるユーザ確認システムの一例を示す構成図。

【図4】同実施形態の動作例を示す流れ図。

【図5】本発明の第3の実施の形態に係る生体データによるユーザ確認システムの一例を示す構成図。

【図6】実施形態の動作例を示す流れ図。

【図7】本発明の第4の実施の形態に係る生体データによるユーザ確認システムの一例を示す構成図。

【図8】同実施形態の動作例を示す流れ図。

【図9】本発明の第5の実施の形態に係る生体データによるユーザ確認システムの一例を示す構成図。

【図10】本発明の第6の実施の形態に係る生体データによるユーザ確認システムの一例を示す構成図。

【図11】本発明の第7の実施の形態に係る生体データによるユーザ確認システムの一例を示す構成図。

【図12】本発明の第8の実施の形態に係る生体データによるユーザ確認システムの一例を示す構成図。

【図13】同実施形態の全体動作を示す流れ図。

【図14】同実施形態における暗号化処理を示す流れ図。

【図15】バイオメトリクスを適用させたICカード署名システムにおける構成要素及びその組み合わせ結果を示す図。

【符号の説明】

1a，1b，1c，1d，1f，1g，1h…センサモジュール

2a，2b，2c，2d，2e，2f，2g，2h…コンピュータ

3a，3b，3c，3d，3e，3g，3h…ICカード

4…インターネット等

5…ハードディスク

11…センサ

12…生体データ保持部

13…照合処理部

14…同定文字列格納部

15…コマンド出力部

16…メッセージ出力部

17…確認処理部

18…同定文字列格納部

19…演算処理部

20…秘密鍵保持部

21…復号処理部

22…復号鍵保持部

23…照合機能部

31a…照合計算部

32a…暗号化生体データ保持部

34…起動対象ソフトウエア

37…暗号化プログラム

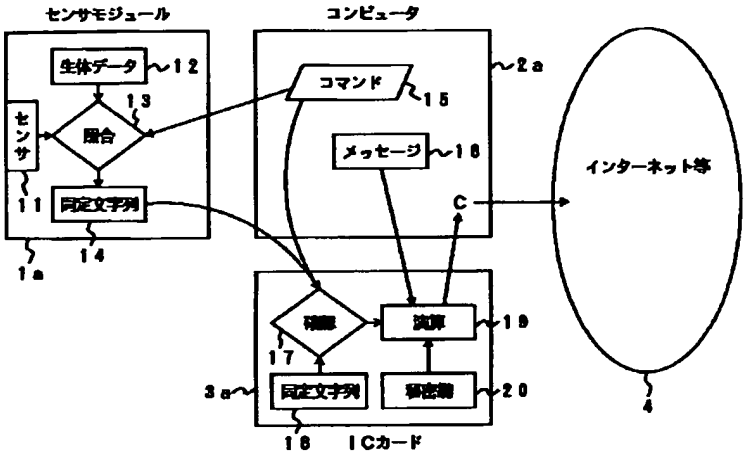
38…暗号計算部

39…暗号鍵保持部

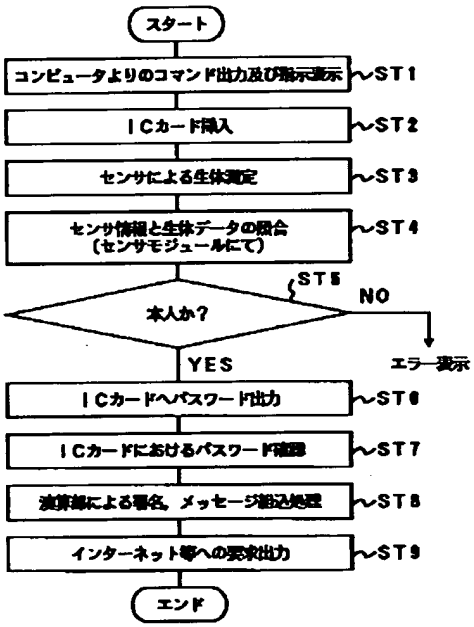
40…入力ファイル

41…出力ファイル

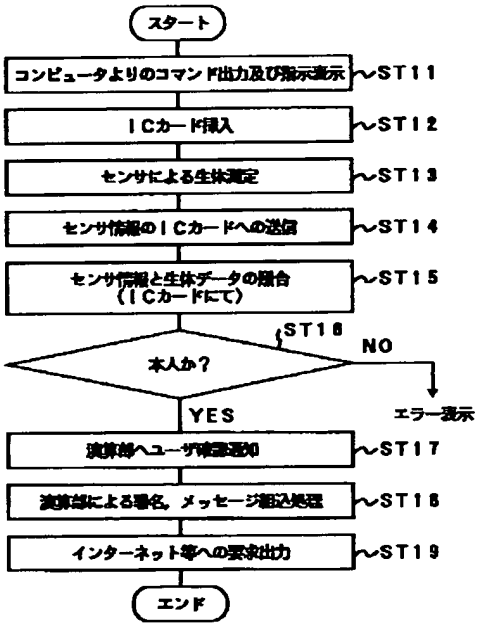
【図1】


センサモジュール
コンピュータ
生体データ
12
13
照合
センサ
11
固定文字列
14
1a
コマンド
15
2a
メッセージ
16
C
インターネット等
確認
演算
19
17
3a
固定文字列
秘密鍵
20
18
ICカード
4

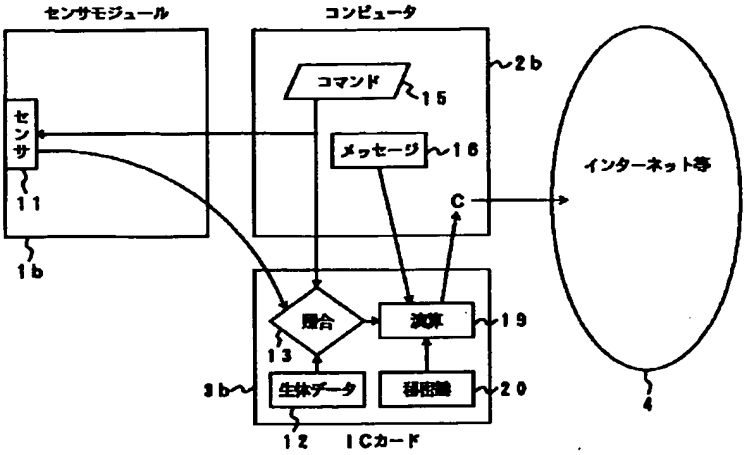
【図2】


スタート
コンピュータよりのコマンド出力及び指示表示
ST1
ICカード挿入
ST2
センサによる生体測定
ST3
センサ情報と生体データの照合
(センサモジュールにて)
ST4
ST5
本人か?
NO
エラー表示
YES
ICカードへパスワード出力
ST6
ICカードにおけるパスワード確認
ST7
演算部による署名、メッセージ組込処理
ST8
インターネット等への要求出力
ST9
エンド

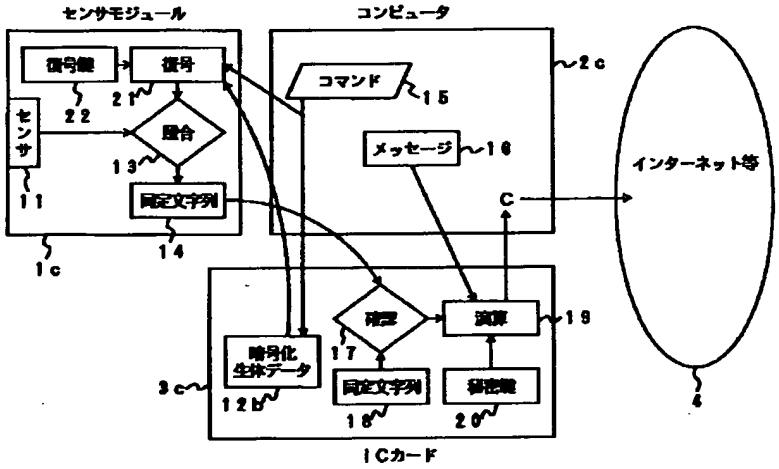
【図4】


スタート
コンピュータよりのコマンド出力及び指示表示
ST11
ICカード挿入
ST12
センサによる生体測定
ST13
センサ情報のICカードへの送信
ST14
センサ情報と生体データの照合
(ICカードにて)
ST15
ST16
本人か?
NO
エラー表示
YES
演算部へユーザ確認通知
ST17
演算部による署名、メッセージ組込処理
ST18
インターネット等への要求出力
ST19
エンド

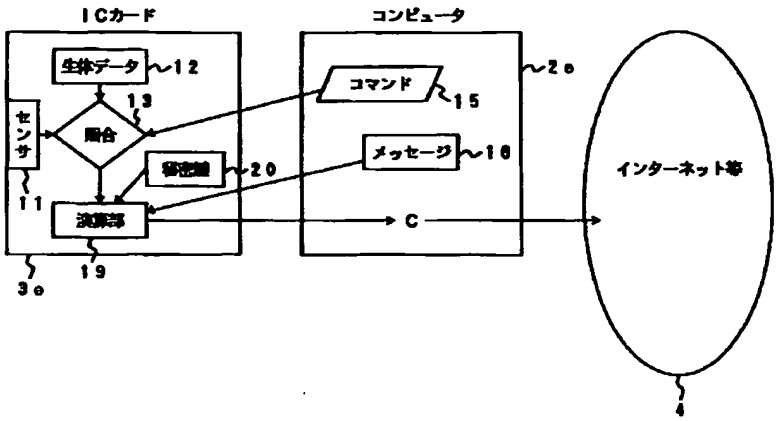
【図3】


センサモジュール
コンピュータ
2b
コマンド
15
センサ
11
メッセージ
16
インターネット等
C
1b
照合
19
13
3b
生体データ
秘密鍵
20
12
ICカード
4

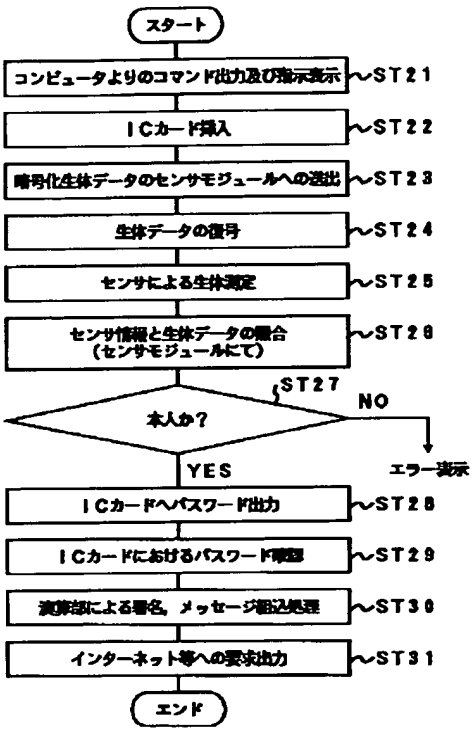
【図5】


センサモジュール
コンピュータ
復号鍵
復号
2c
コマンド
15
22
21
センサ
照合
メッセージ
16
インターネット等
13
11
同定文字列
C
14
1c
暗号化
生体データ
19
17
3c
12b
同定文字列
秘密鍵
18
20
ICカード
4

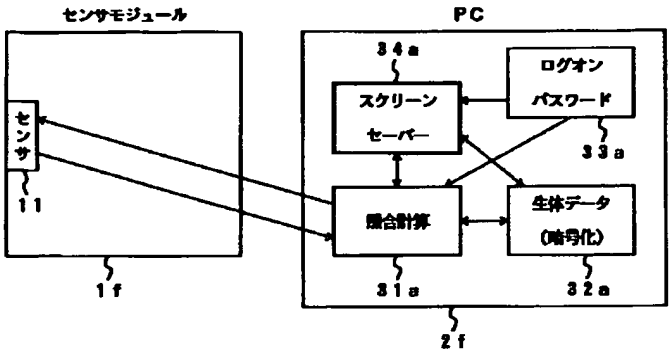
【図9】


ICカード
コンピュータ
生体データ
12
2e
コマンド
15
13
センサ
照合
メッセージ
16
秘密鍵
20
インターネット等
11
演算部
C
19
3e
4

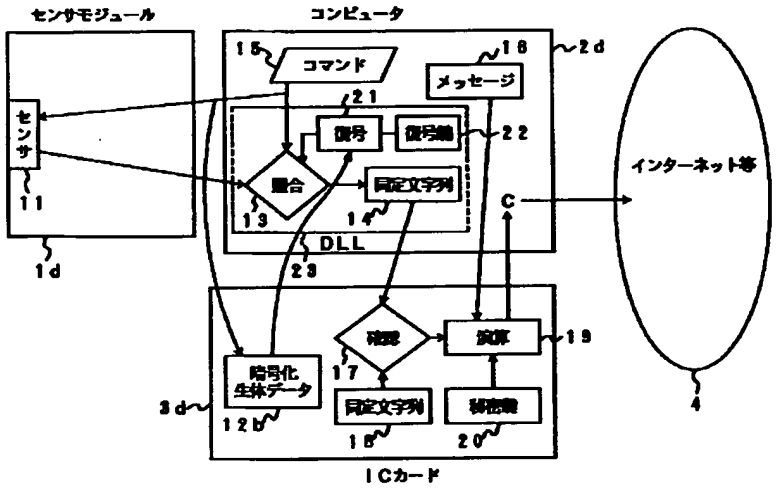
【図6】


スタート
コンピュータよりのコマンド出力及び指示表示
ST21
ICカード挿入
ST22
暗号化生体データのセンサモジュールへの送出
ST23
生体データの復号
ST24
センサによる生体測定
ST25
センサ情報と生体データの照合
(センサモジュールにて)
ST26
ST27
本人か?
NO
エラー表示
YES
ICカードへパスワード出力
ST28
ICカードにおけるパスワード確認
ST29
演算部による署名、メッセージ組込処理
ST30
インターネット等への要求出力
ST31
エンド

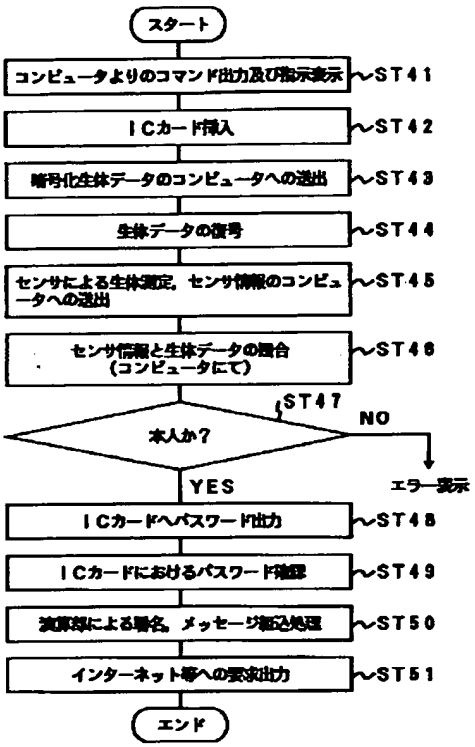
【図10】


センサモジュール
PC
センサ
11
1f
34a
スクリーンセーバー
ログオンパスワード
33a
照合計算
生体データ(暗号化)
31a
32a
2f

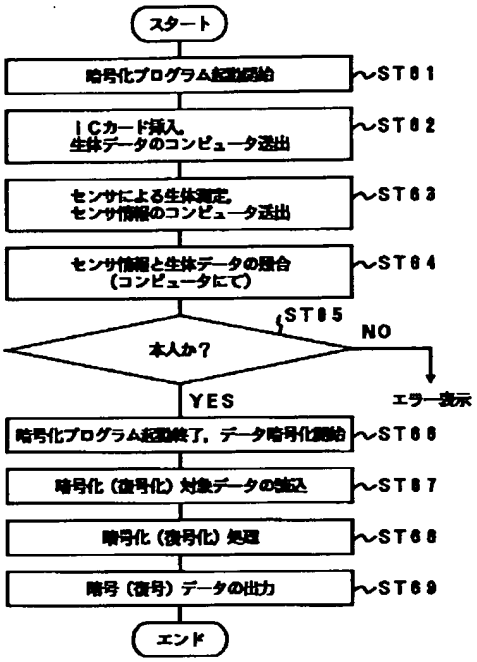
【図7】


センサモジュール
コンピュータ
センサ
11
1d
15
コマンド
16
メッセージ
2d
21
復号
復号鍵
22
照合
同定文字列
13
14
DLL
23
C
インターネット等
4
確認
演算
17
19
暗号化生体データ
3d
12b
同定文字列
18
秘密鍵
20
ICカード

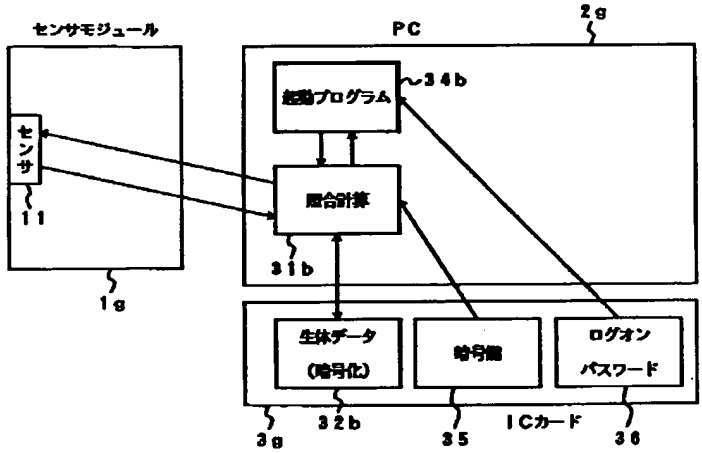
【図8】


スタート
コンピュータよりのコマンド出力及び指示表示
ST41
ICカード挿入
ST42
暗号化生体データのコンピュータへの送出
ST43
生体データの復号
ST44
センサによる生体測定，センサ情報のコンピュータへの送出
ST45
センサ情報と生体データの照合（コンピュータにて）
ST46
ST47
本人か？
NO
エラー表示
YES
ICカードへパスワード出力
ST48
ICカードにおけるパスワード確認
ST49
演算部による署名，メッセージ転送処理
ST50
インターネット等への要求出力
ST51
エンド

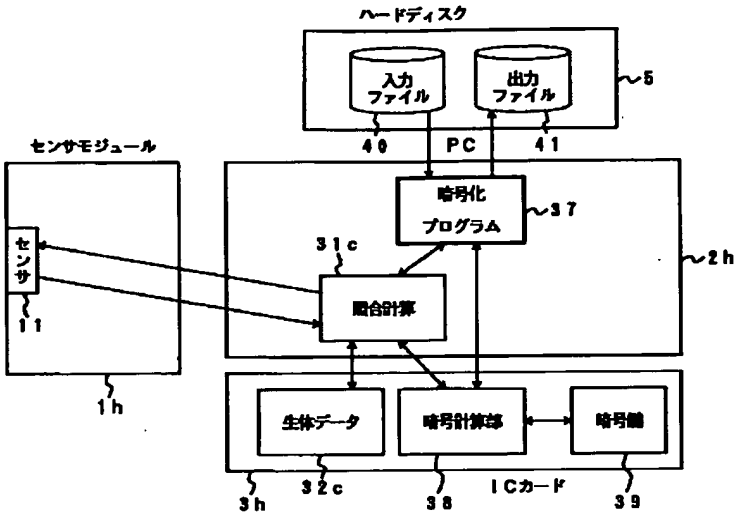
【図13】


スタート
暗号化プログラム起動開始
ST61
ICカード挿入，生体データのコンピュータ送出
ST62
センサによる生体測定，センサ情報のコンピュータ送出
ST63
センサ情報と生体データの照合（コンピュータにて）
ST64
ST65
本人か？
NO
エラー表示
YES
暗号化プログラム起動終了，データ暗号化開始
ST66
暗号化（復号化）対象データの読込
ST67
暗号化（復号化）処理
ST68
暗号（復号）データの出力
ST69
エンド

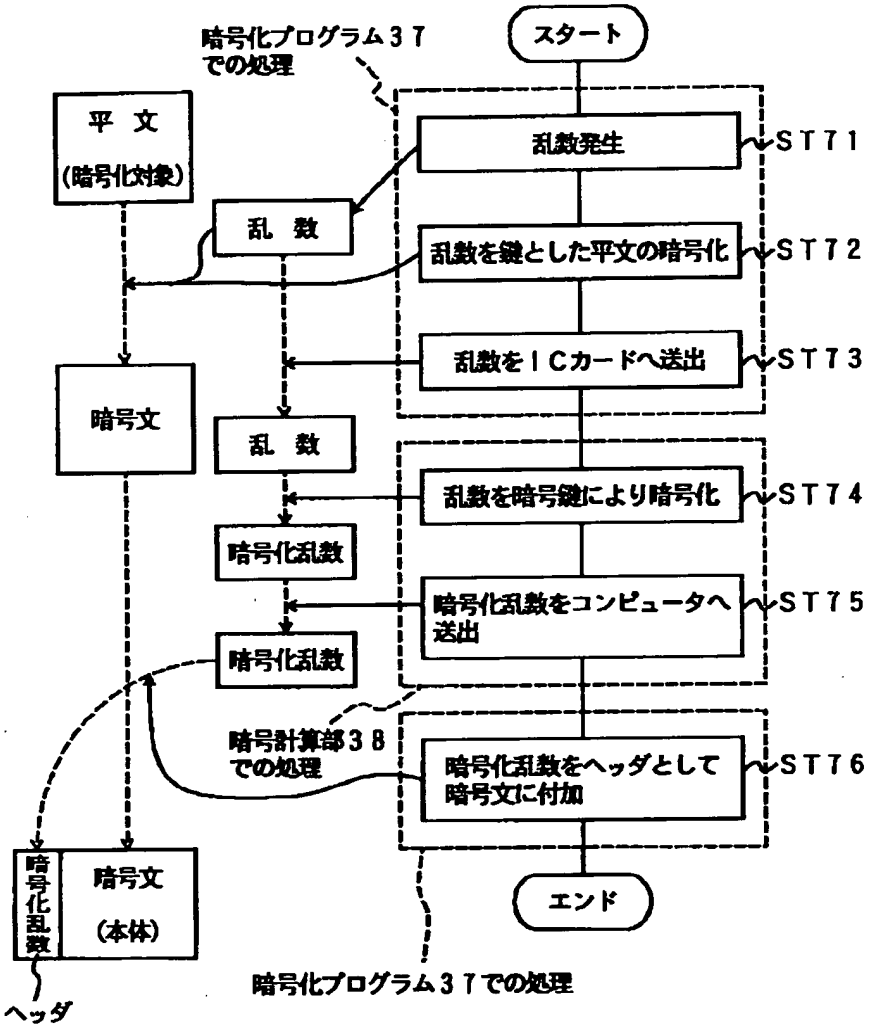
【図11】


センサモジュール
PC
2g
起動プログラム
34b
センサ
11
照合計算
31b
1g
生体データ（暗号化）
暗号鍵
ログオンパスワード
3g
32b
35
ICカード
36

【図12】


ハードディスク
入力ファイル
出力ファイル
5
40
PC
41
センサモジュール
暗号化プログラムA
37
31c
センサ
11
照合計算
2h
1h
生体データ
暗号計算部
暗号鍵
3h
32c
38
ICカード
39

【図14】


暗号化プログラム37での処理
スタート
平 文
(暗号化対象)
乱数発生
ST71
乱 数
乱数を鍵とした平文の暗号化
ST72
乱数をICカードへ送出
ST73
暗号文
乱 数
乱数を暗号鍵により暗号化
ST74
暗号化乱数
暗号化乱数をコンピュータへ送出
ST75
暗号化乱数
暗号計算部38での処理
暗号化乱数をヘッダとして暗号文に付加
ST76
暗号化乱数
暗号文
(本体)
エンド
ヘッダ
暗号化プログラム37での処理

【図15】

	候補システム	ICカード	センサ	PC&R/W	サーバー	照合装置のタイプ	備　考
第5実施形態	ICカード一体型	生体，照合				1チップ	理想的
第1実施形態	耐タンパーモジュール一体型	PIN	PIN，生体，照合			1チップ，スタンドアロン	従来カード利用可
第2実施形態	万能ICカード型	生体，照合				従来型	準理想的
第3実施形態	ICカードにデーターセンサ計算型	生体	照合			スタンドアロン	一般的，カードに機能付加要
第4実施形態	ICカードにデーターPC計算型	生体，文字列		文字列，照合		従来型	一般的，カードに機能付加要，依頼計算の検討要
	（参考例1）	生体			照合	従来型	一般的，カードに機能付加要
	（参考例2）		生体	照合		メモリ内蔵型	変形例，従来カード利用可
	（参考例3）		生体		照合	メモリ内蔵型	変形例，従来カード利用可
	（参考例4）	照合	生体			メモリ内蔵型	変形例
	（参考例5）				生体，照合	従来型	従来カード利用可
	（参考例6）			生体（暗号化），照合		従来型	従来カード利用可

生体データと照合計算の配置可能性